

# OBSERVABILITY AND DIAGNOSABILITY OF FINITE STATE SYSTEMS: A UNIFYING FRAMEWORK

ELENA DE SANTIS AND MARIA D. DI BENEDETTO

**ABSTRACT.** In this paper, a general framework is proposed for the analysis and characterization of observability and diagnosability of finite state systems. Observability corresponds to the reconstruction of the system's discrete state, while diagnosability corresponds to the possibility of determining the past occurrence of some particular states, for example faulty states. A unifying framework is proposed where observability and diagnosability properties are defined with respect to a critical set, i.e. a set of discrete states representing a set of faults, or more generally a set of interest. These properties are characterized and the involved conditions provide an estimation of the delay required for the detection of a critical state, of the precision of the delay estimation and of the duration of a possible initial transient where the diagnosis is not possible or not required. Our framework makes it possible to precisely compare some of the observability and diagnosability notions existing in the literature with the ones introduced in our paper, and this comparison is presented.

## 1. INTRODUCTION

Reconstructing the internal behavior of a dynamical system on the basis of the available measurements is a central problem in control theory. Starting from the seminal paper [15], state observability has been investigated both in the continuous domain (see e.g. the fundamental papers [19] for the linear case and [13] for the nonlinear case), in the discrete state domain (see e.g. [20] and [23]), and more recently for hybrid systems (see e.g. the special issue [10] on observability and observer-based control of hybrid systems and the references therein, [3], [4], [6], [1], [9], [31], [2], [30]). In some references dealing with discrete event systems, e.g. in [16], the notion of observability is related to state disambiguation, which is the property of distinguishing unambiguously among certain pairs of states in the state space. We will use here the term observability in the traditional meaning used in [35] where observability corresponds to the reconstruction of the system's discrete state. Diagnosability, a property that is closely related to observability but is more general, corresponds to the possibility of detecting the occurrence of some particular state, for example a faulty state, on the basis of the observations. An excellent survey of recent advances on diagnosis methods for discrete systems can be found in [35]. The formal definition and analysis of observability and diagnosability depend on the model, on the available output information, and on the objective for which state reconstruction is needed, e.g. for control purposes, for detection of critical situations, and for diagnosis of past system evolutions. It is therefore hard, in general, to understand the precise relationships that exist between the different notions that exist in the literature.

In this paper, we propose a unifying framework where observability and diagnosability are defined with respect to a subset of the state space, called critical set. A state belonging to the critical set is called critical state. This idea comes from safety critical applications, e.g. Air Traffic Management [12], [8], where the critical set of discrete states represents dangerous situations that must be detected to avoid unsafe or even catastrophic behavior of the system. However, the critical set can represent a set of faults, or more generally any set of interest. We define and characterize observability and diagnosability in a uniform set-membership-based formalism. The set-membership formalism and the derived algorithms are very simple and intuitive, and allow checking the properties without constructing an observer, thereby avoiding the exponential complexity of the observer design. The definitions of observability and diagnosability are given in a general form that is

---

The research leading to these results has been partially supported by the Center of Excellence DEWS.

parametric with respect to the delay required for the detection of a critical state, and the precision of the delay estimation. Using the proposed conditions that characterize those properties, we can check diagnosability of a critical event, such as a faulty event, and at the same time compute the delay of the diagnosis with respect to the occurrence of the event, the uncertainty about the time at which that event occurred, and the duration of a possible initial transient where the diagnosis is not possible or not required. These evaluations are useful to better understand the characteristics of the system and can be used in the implementation of the diagnoser.

While in the literature on discrete event systems a transition-based model is used, we adopt a state-based approach, similarly to what was done in [17] where an on-line diagnosability problem for a deterministic Moore automaton with partial state observation was solved, in [14] where the focus was on the complexity reduction in the diagnoser design, and in [29] where verification of codiagnosability is performed. Because of the different formalism used in the transition-based and state-based approaches, a comparison between our definitions and those existing in the literature on discrete event systems is very hard to achieve without a unifying framework where the different notions can all be formulated and compared. We show that, using our formalism, we are able to understand the precise relationships that exist between the properties we analyze and some of the many diagnosability concepts that exist in the literature.

The paper is organized as follows. After introducing the main definitions in Section 2, Section 3 is devoted to establishing some geometrical tools that are instrumental in proving our results. In Section 4, observability and diagnosability properties are completely characterized. The proofs of the main theorems are constructive and show how a diagnoser can be determined. Some examples are described in Section 5. Finally, in the Appendix we present an extension of some results of the paper under milder technical assumptions.

**Notations:** The symbol  $\mathbb{Z}$  denotes the set of nonnegative integer numbers. For  $a, b \in \mathbb{Z}$ ,  $[a, b]$  denotes the set  $[a, b] = \{x \in \mathbb{Z} : a \leq x \leq b\}$ . For a set  $X$ , the symbol  $|X|$  denotes its cardinality. For a set  $Y \subset X$ , where the symbol  $\subset$  has to be understood as "subset", not necessarily strict, the symbol  $\bar{Y}$  denotes the complement of  $Y$  in  $X$ , i.e.  $\bar{Y} = \{x \in X : x \notin Y\}$ . For  $W \subset X \times X$ , the symbol  $W^-$  denotes the symmetric closure of  $W$ , i.e.  $W^- = \{(x_1, x_2) : (x_1, x_2) \in W \text{ or } (x_2, x_1) \in W\}$ . The null event is denoted by  $\epsilon$ . For a string  $\sigma$ ,  $|\sigma|$  denotes its length,  $\sigma(i)$ ,  $i \in \{1, 2, \dots, |\sigma|\}$ , denotes the  $i$ -th element, and  $|\sigma|_{[a,b]}$  is the string  $\sigma(a)\sigma(a+1)\dots\sigma(b)$ .  $P(\sigma)$  is the projection of the string  $\sigma$ , i.e. the string obtained from  $\sigma$  by erasing the symbol  $\epsilon$  (see e.g. [22]). In all figures, the cardinal number inside the circle denotes the state, the lowercase letter besides the same circle denotes the output associated to that state.

## 2. DIAGNOSABILITY PROPERTIES AND THEIR RELATIONSHIPS

We consider a Finite State Machine (FSM)

$$M = (X, X_0, Y, H, \Delta)$$

where:

- $X$  is the finite set of states;
- $X_0 \subset X$  is the set of initial states;
- $Y$  is the finite set of outputs;
- $H : X \rightarrow Y$  is the output function;
- $\Delta \subset X \times X$  is the transition relation.

For  $i \in X$ , define  $\text{succ}(i) = \{j \in X : (i, j) \in \Delta\}$  and  $\text{pre}(i) = \{j \in X : (j, i) \in \Delta\}$ .

We make the following standard assumption:

**Assumption 1:** (liveness)  $\text{succ}(i) \neq \emptyset, \forall i \in X$ .

Any finite or infinite string  $x$  with symbols in  $X$  that satisfies the condition

$$(2.1) \quad \begin{aligned} & x(1) \in X \\ & x(k+1) \in \text{succ}(x(k)), \quad k = 1, 2, \dots, |x| - 1 \end{aligned}$$

is called a state execution (or state trajectory or state evolution) of the FSM  $M$ . The singleton  $\{i \in X\}$  is an execution.

Let  $\mathcal{X}^*$  be the set of all the state executions of  $M$ . Then, for a given  $\Psi \subset X$ , we can define the following subsets of  $\mathcal{X}^*$ :

- $\mathcal{X}_\Psi$  is the set of state executions  $x \in \mathcal{X}^*$  with  $x(1) \in \Psi$
- $\mathcal{X}_{\Psi, \infty}$  is the set of infinite state executions  $x \in \mathcal{X}^*$  with  $x(1) \in \Psi$ . For simplicity, the set  $\mathcal{X}_{X_0, \infty}$  will be denoted by  $\mathcal{X}$
- $\mathcal{X}^\Psi$  is the set of finite state executions  $x \in \mathcal{X}^*$  with last symbol in  $\Psi$

Obviously,

$$\mathcal{X}_X = \mathcal{X}^*$$

and

$$\mathcal{X}_{\Psi, \infty} \subset \mathcal{X}_\Psi \subset \mathcal{X}^*$$

Let  $\mathcal{Y}$  be the set of strings with symbols in  $\hat{Y} = \{y \in Y : y \neq \epsilon\}$ . Define  $\mathbf{y} : \mathcal{X}^* \rightarrow \mathcal{Y}$ , the function that associates to a state execution the corresponding output execution, as

$$\mathbf{y}(x) = P(\sigma)$$

where

$$\sigma = H(x(1)) \dots H(x(n)), n = |x|$$

if  $|x|$  is finite. Otherwise

$$\mathbf{y}(x) = P(\sigma_\infty)$$

where  $\sigma_\infty$  is an infinite string recursively defined as

$$\begin{aligned} \sigma_1 &= H(x(1)) \\ \sigma_{k+1} &= \sigma_k H(x(k+1)), \quad k = 1, 2, \dots \end{aligned}$$

Finally, for  $x \in \mathcal{X}_{X_0}$

$$\mathbf{y}^{-1}(\mathbf{y}(x)) = \{\hat{x} \in \mathcal{X}_{X_0} : \mathbf{y}(\hat{x}) = \mathbf{y}(x)\}$$

We now propose a framework where observability and diagnosability are defined with respect to a subset of the state space  $\Omega \subset X$  called critical set. The set  $\Omega$  may represent unsafe states, faulty states, or more generally any set of states of interest.

For a string  $x \in \mathcal{X}$ , two cases are possible:

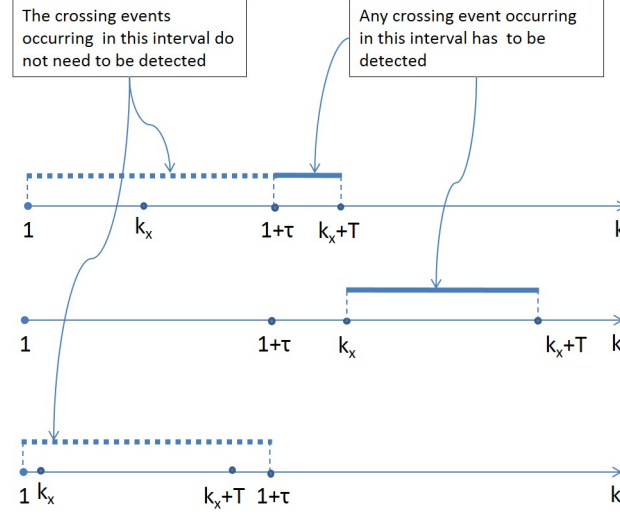
- i)  $x(k) \notin \Omega, \forall k \in \mathbb{Z}$
- ii)  $x(k) \in \Omega$ , for some  $k \in \mathbb{Z}$

If the second condition holds, let  $k_x$  be the minimum value of  $k$  such that  $x(k) \in \Omega$ , i.e.

$$(2.2) \quad \begin{aligned} & k_x = k \in \mathbb{Z} : x(k) \in \Omega \\ & \text{and} \\ & (k = 1 \text{ or } x(h) \notin \Omega, \forall h \in [1, k-1]) \end{aligned}$$

Otherwise set  $k_x = \infty$ .

The next definition describes the capability of inferring, from the output execution, that the state belongs to the set  $\Omega$ , at some step during the execution, after a finite transient or after a finite delay or with some

FIGURE 1. Illustration of parameters  $k_x$ ,  $\tau$  and  $T$ 

uncertainty in the determination of the step. The precise meaning of the parameters used to describe those characteristics will be discussed after the definition.

**Definition 2.1.** The FSM  $M$  is parametrically diagnosable with respect to a set  $\Omega \subset X$  (shortly parametrically  $\Omega$  – *diag*) if there exist  $\tau$  and  $\delta \in \mathbb{Z}$ , and  $T \in \mathbb{Z} \cup \{\infty\}$  such that for any string  $x \in \mathcal{X}$  with finite  $k_x$ , whenever  $x(k) \in \Omega$  and  $k \in [\max\{k_x, (\tau + 1)\}, k_x + T]$ , it follows that for any string  $\hat{x} \in \mathbf{y}^{-1}\left(\mathbf{y}\left(x|_{[1, k+\delta]}\right)\right)$ ,  $\hat{x}(h) \in \Omega$ , for some  $h \in [\max\{1, (k - \gamma_1)\}, k + \gamma_2]$  and for some  $\gamma_1, \gamma_2 \in \mathbb{Z}$ ,  $\gamma_2 \leq \delta$ .

If  $x(k) \in \Omega$  for some  $k \in \mathbb{Z}$ , in what follows the condition  $x(k) \in \Omega$  is called *crossing event*, and  $k$  is the step at which the crossing event occurs.

The value  $\gamma = \max\{\gamma_1, \gamma_2\}$  is the uncertainty radius in the reconstruction of the step at which the crossing event occurred. The parameter  $\delta$  corresponds to the delay of the crossing event detection while  $\tau$  corresponds to an initial time interval where the crossing event is not required to be detected.

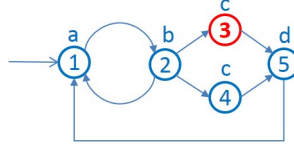
The detection of the crossing event is required whenever it occurs in the interval defined by the parameter  $T$ .

To better understand the role of these parameters, consider the examples in Figure 1. For fixed values  $\tau$ ,  $T$ ,  $\delta$  and  $\gamma$ , we have represented three possible cases, corresponding to three different executions, and hence with different values for  $k_x$ . In the first case  $\max\{k_x, (\tau + 1)\} = (\tau + 1)$ . Hence, any crossing event occurring in  $[(\tau + 1), k_x + T]$  has to be detected, with maximum delay  $\delta$  and with maximum uncertainty  $\gamma$ . Crossing events occurring in  $[1, \tau]$  are not needed to be detected. In the second case,  $\max\{k_x, (\tau + 1)\} = k_x$ , and therefore any crossing event up to step  $k_x + T$  has to be detected, with maximum delay  $\delta$  and with maximum uncertainty  $\gamma$ . Finally in the last case no detection is required.

Obviously  $T = 0$  and  $\tau = 0$  mean that only the first crossing event has to be detected. Moreover,  $\delta = 0$  implies  $\gamma = 0$ , but  $\gamma = 0$  does not imply in general  $\delta = 0$ .

**Example 2.2.** As an example, the FSM in Figure 2, where  $\Omega = \{3\}$ , is not parametrically  $\Omega$  – *diag*: in fact for any  $\tau$  there exists a state execution that crosses the set  $\Omega$  for the first time at some  $k > \tau$ , and it is not possible to detect the crossing event neither immediately nor with delay, neither exactly nor with uncertainty.

By definition of parametric diagnosability, the following monotonicity property holds:

FIGURE 2. The FSM is not parametrically  $\{3\}$  – *diag*.

**Proposition 2.3.** *If  $M$  is parametrically  $\Omega$  – *diag* with parameters  $\tau, \delta, T, \gamma_1, \gamma_2$  then it is parametrically  $\Omega$  – *diag* with parameters  $\tau', \delta', T', \gamma'_1, \gamma'_2$ , where  $\tau' \geq \tau, \delta' \geq \delta, T' \leq T, \gamma'_1 \geq \gamma_1, \gamma'_2 \geq \gamma_2, \gamma'_2 \leq \delta'$ .*

Depending on the values taken by  $\tau, \delta$  and  $T$ , special instances of Definition 2.1 are obtained. We consider the following, which highlight the role of these parameters:

$$(2.3) \quad \begin{array}{lll} a. & T = 0 & \tau = 0 \quad \delta \geq 0 \\ b. & T = \infty & \tau > 0 \quad \delta > 0 \\ c. & T = \infty & \tau > 0 \quad \delta = 0 \\ d. & T = \infty & \tau = 0 \quad \delta > 0 \\ e. & T = \infty & \tau = 0 \quad \delta = 0 \end{array}$$

**case a.:** Since  $T = 0$  the crossing event can be detected the first time it occurs, immediately or with some delay. If  $\Omega \subset X_0$ , and  $\gamma_1 = \gamma_2 = 0$ , case a. becomes an extension of the definition of initial state observability property, as given e.g. in [23], which we call here  $\Omega$ –*initial state observability*.

**case b.:** In this case, the crossing event can be detected with a maximum delay of  $\delta$  steps whenever it occurs for  $k \geq \tau + 1$ . However, since  $\tau \geq 1$ , the event  $x(k) \in \Omega, k \in [1, \tau]$  may not be detected (in this case, parametric diagnosability is an "eventual" property). The notion of  $(k_1, k_2)$ –*detectability*, as introduced in [27] can be retrieved as a special case. In fact it corresponds to parametric  $\{x\}$ –diagnosability,  $\forall x \in X$ , with parameters  $T = \infty, \tau = k_1, \delta = k_2$  and  $\gamma = 0$ .

**case c.:** With respect to case b., in this case the crossing event can be detected without any delay, and the FSM  $M$  is said to be  $\Omega$ –*current state observable*. It is again an "eventual" property. Moreover,  $M$  is said to be *current state observable* if it is  $\{x\}$ –current state observable,  $\forall x \in X$ . The notion of current state observability coincides with the one studied in [2] and with the notion of Strong Detectability as defined in [28]. Finally, if  $\Omega = \{x\}$  and  $M$  is  $\Omega$ –current state observable, then the state  $x$  is *always observable*, as defined in [20].

**case d.:** The meaning is the same as in case b., but with  $\tau = 0$ . In this case, the FSM  $M$  is said to be *critically diagnosable* with respect to  $\Omega$  (critical  $\Omega$  – *diag*). Critical diagnosability is an "always" property.

**case e.:** The meaning is the same as in case c., but with  $\tau = 0$ . The FSM  $M$  is said to be *critically observable* with respect to  $\Omega$  (critical  $\Omega$  – *obs*). It is again an "always" property. The notion of critical observability for an FSM was introduced in [11] and [12]. In [8] the same notion was extended to linear switching systems with minimum and maximum dwell time. Finally, in [21] the analysis of critical observability was extended to the case of networks of Finite State Machines.

For an exhaustive analysis, in addition to the cases above, let's consider also the case when  $T$  is finite and nonzero. This case deserves some attention only if we require the exact reconstruction of the step at which the crossing event occurs, i.e.  $\gamma = 0$ . In fact, if  $M$  is parametrically  $\Omega$  – *diag* with parameters  $\tau, \delta, T = 0, \gamma_1, \gamma_2$ , then, by Definition 2.1 and by Proposition 2.3 it is parametrically  $\Omega$  – *diag* also with parameters  $\tau + \hat{T}, \delta + \hat{T}, T = \hat{T}, \gamma_1 + \hat{T}, \gamma_2 + \hat{T}$ , for any finite  $\hat{T} \in \mathbb{Z}$ . Conversely, by Definition 2.1, if  $M$  is parametrically  $\Omega$  – *diag* with parameters  $\tau, \delta, T = \hat{T}, \gamma_1, \gamma_2$  then it is  $\Omega$  – *diag* also with parameters  $\tau, \delta, T = 0, \gamma_1, \gamma_2$ . The characterization of the property in the case  $T$  finite and nonzero and  $\gamma = 0$  is a generalization of case a, which is not explicitly addressed in this paper.

For simplicity of exposition, we now define three properties that correspond to case *a.*, cases *b.* and *c.*, cases *d.* and *e.*, respectively.

**Definition 2.4.** (case *a.*) The FSM  $M$  is *diagnosable* with respect to a set  $\Omega \subset X$  ( $\Omega - diag$ ) if there exists  $\delta \in \mathbb{Z}$ , such that for any  $x \in \mathcal{X}$  for which  $k_x \neq \infty$ , it follows that for any string  $\hat{x} \in \mathbf{y}^{-1}\left(\mathbf{y}\left(x|_{[1, k_x + \delta]}\right)\right)$ ,  $\hat{x}(h) \in \Omega$ , for some  $h \in [\max\{1, k_x - \gamma_1\}, k_x + \gamma_2]$  and for some  $\gamma_1, \gamma_2 \in \mathbb{Z}$ ,  $\gamma_2 \leq \delta$ . If the property holds with  $\delta = 0$ ,  $M$  will be called *observable* with respect to a set  $\Omega \subset X$  ( $\Omega - obs$ ). If  $\Omega \subset X_0$  and the property holds with  $\gamma_1 = \gamma_2 = 0$ ,  $M$  will be called  *$\Omega$ -initial state observable*.

The  $\Omega - diag$  property of Definition 2.4 corresponds to the one given in [25], where only the detection of the condition  $x(h) \in \Omega$ , for some  $h \in [1, k_x + \delta]$ , is required but not the refinement of the identification of the step at which the crossing event occurs. However, we will show in Section 4.2 that these two properties are equivalent, i.e. an FSM enjoys the property in [25] if and only if the requirements of Definition 2.4 hold.

**Definition 2.5.** (cases *b.* and *c.*) The FSM  $M$  is *eventually diagnosable* with respect to a set  $\Omega \subset X$  (eventually  $\Omega - diag$ ) if there exist  $\tau$  and  $\delta \in \mathbb{Z}$  such that for any string  $x \in \mathcal{X}$  with finite  $k_x$ , whenever  $x(k) \in \Omega$  and  $k \geq \max\{k_x, (\tau + 1)\}$ , it follows that for any string  $\hat{x} \in \mathbf{y}^{-1}\left(\mathbf{y}\left(x|_{[1, k + \delta]}\right)\right)$ ,  $\hat{x}(h) \in \Omega$ , for some  $h \in [\max\{1, k - \gamma_1\}, k + \gamma_2]$  and for some  $\gamma_1, \gamma_2 \in \mathbb{Z}$ ,  $\gamma_2 \leq \delta$ . If the condition holds with  $\delta = 0$ ,  $M$  will be called *eventually observable* with respect to a set  $\Omega \subset X$  (eventually  $\Omega - obs$ ).

Finally, we state the following definition

**Definition 2.6.** (cases *d.* and *e.*) The FSM  $M$  is *critically diagnosable* with respect to a set  $\Omega \subset X$  (critically  $\Omega - diag$ ) if there exists  $\delta \in \mathbb{Z}$ , such that for any string  $x \in \mathcal{X}$  with finite  $k_x$ , whenever  $x(k) \in \Omega$ , it follows that for any string  $\hat{x} \in \mathbf{y}^{-1}\left(\mathbf{y}\left(x|_{[1, k + \delta]}\right)\right)$ ,  $\hat{x}(h) \in \Omega$ , for some  $h \in [\max\{1, k - \gamma_1\}, k + \gamma_2]$ , and for some  $\gamma_1, \gamma_2 \in \mathbb{Z}$ ,  $\gamma_2 \leq \delta$ . If the condition holds with  $\delta = 0$ , the FSM  $M$  is called *critically observable* with respect to  $\Omega \subset X$  (critically  $\Omega - obs$ ).

The following relationship can be established between the diagnosability properties introduced above.

**Proposition 2.7.**  $M$  is critically  $\Omega - diag$  if and only if it is  $\Omega - diag$  and eventually  $\Omega - diag$ .

*Proof.* The necessity is obvious. Sufficiency: suppose that  $M$  is eventually  $\Omega - diag$  with parameters  $\gamma'_1, \gamma'_2, \tau'$  and  $\delta'$  and that it is  $\Omega - diag$  with parameter  $\delta''$ . Then,  $M$  is eventually  $\Omega - diag$  with parameters  $\tau = 0, \delta = \max\{\tau', \delta', \delta''\}, \gamma_1 = \max\{\tau', \gamma'_1\}, \gamma_2 = \delta = \max\{\tau', \delta', \delta''\}$ , and hence it is critically  $\Omega - diag$ .  $\square$

We will characterize the properties in Definitions 2.1, 2.4 and 2.5. The characterization of the property in Definition 2.6 will follow by Proposition 2.7 as a simple corollary.

*Remark 2.8.* If  $X_0 = X$  and  $\tau = \delta = 0$ , Definitions 2.4 and 2.5 become trivial since they correspond in that case to an instantaneous detection of the crossing event, i.e.  $H(i) \neq H(j), \forall i, j$  such that  $i \in \Omega$  and  $j \notin \Omega$ .

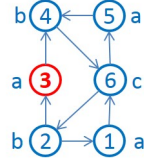
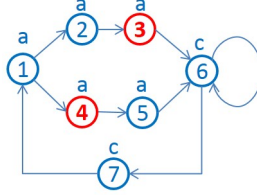
We end this section with two examples. The first is an FSM  $M$  which is eventually  $\Omega - diag$ , with  $\tau = 1, \delta = 1$ , but not with  $\tau = 0$  or  $\delta = 0$ . The second shows an FSM which is eventually  $\Omega - diag$ , with  $\tau = 1, \delta = 2, \gamma = 1$ , but not with  $\tau = 1, \delta = 2$  and  $\gamma = 0$ .

**Example 2.9.** Let  $M = (X, X_0, Y, H, \Delta)$ ,  $X = X_0 = \{1, 2, 3, 4, 5, 6\}$ ,  $Y = \{a, b, c\}$ ,  $H(1) = H(3) = H(5) = a$ ,  $H(2) = H(4) = b$ ,  $H(6) = c$ ,

$$\Delta = \{(1, 6), (2, 1), (2, 3), (6, 2), (3, 4), (4, 6), (5, 4), (6, 5)\}$$

be represented in Figure 3.

Let  $\Omega = \{3\}$ .  $M$  is not eventually  $\Omega - diag$ , with  $\delta = 0$ . In fact for any state execution ending in state 3 there is a state execution ending in state 1, with the same output string.  $M$  is not eventually  $\Omega - diag$ , with  $\tau = 0$ .

FIGURE 3. FSM  $M$  (Example 2.9).FIGURE 4. FSM  $M$  (Example 2.10).

In fact for any state execution starting from 3 there is a state execution starting from 5, with the same output string.  $M$  is eventually  $\Omega$ -diag, with  $\tau = 1$ ,  $\delta = 1$  and  $\gamma = 0$ : in fact any output finite string ending with the string "bab" allows the detection of the crossing event and the step at which the crossing occurred.

**Example 2.10.** Let  $M = (X, X_0, Y, H, \Delta)$ ,  $X = X_0 = \{1, 2, 3, 4, 5, 6, 7\}$ ,  $Y = \{a, c\}$ ,  $H(i) = a$ ,  $i = 1 \dots 5$ ,  $H(i) = c$ ,  $i = 6, 7$  and  $\Delta$  equal to the set

$$\{(1, 2), (2, 3), (3, 6), (1, 4), (4, 5), (5, 6), (6, 6), (6, 7), (7, 1)\}$$

be represented in Figure 4.

Let  $\Omega = \{3, 4\}$ . By inspection, we see that  $M$  is eventually  $\Omega$ -diag, with  $\tau = 1$ ,  $\delta = 2$ ,  $\gamma_1 = 1$  and  $\gamma_2 = 1$ . It is not eventually  $\Omega$ -diag with  $\gamma_1 = 0$  and  $\gamma_2 = 0$ . This means that it is possible to detect the crossing event, but not the step at which the crossing occurred. Note that if  $X_0 = \{1, 2, 4\}$ , then  $M$  is eventually  $\Omega$ -diag, with  $\tau = 0$ ,  $\delta = 2$ ,  $\gamma_1 = 1$  and  $\gamma_2 = 1$ , and hence it is critically  $\Omega$ -diag.

### 3. INDISTINGUISHABILITY NOTIONS

In what follows, we will assume that the set of outputs does not contain the null event  $\epsilon$ .

**Assumption 2::**  $\epsilon \notin Y$ .

If an FSM  $M$  with  $\epsilon \in Y$  is such that any cycle has at least a state  $i$  with  $H(i) \neq \epsilon$ , then we can define an FSM  $\widehat{M}$  with  $\epsilon \notin Y$  such that checking the parametric diagnosability property for  $M$  is equivalent to checking the parametric diagnosability property for  $\widehat{M}$ . The parameters for which the two properties are satisfied will in general be different for  $M$  and  $\widehat{M}$ . Details about this equivalence can be found in the Appendix.

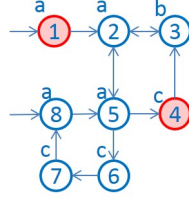
Given the FSM  $M = (X, X_0, Y, H, \Delta)$  and the set  $\Omega$ , define the sets

$$\Pi = \{(i, j) \in X \times X : H(i) = H(j)\}$$

and

$$\Theta = \{(i, j) \in X \times X : i = j\} \subset \Pi$$

By definition, the set  $\Pi$  and all its subsets are symmetric.

FIGURE 5. FSM  $M$  (Example 3.3).

We will refer to the following indistinguishability notions.

**Definition 3.1.** Two state trajectories  $x_1$  and  $x_2$  in  $\mathcal{X}^*$  are called indistinguishable if  $\mathbf{y}(x_1) = \mathbf{y}(x_2)$ . The pair  $(i, j) \in \Pi$  is  $k$ -forward indistinguishable if there exist  $x_1 \in \mathcal{X}_{\{i\}}$  and  $x_2 \in \mathcal{X}_{\{j\}}$ , such that  $|x_1| = |x_2| = k$  and  $\mathbf{y}(x_1) = \mathbf{y}(x_2)$ . The pair  $(i, j) \in \Sigma \subset \Pi$  is  $k$ -backward indistinguishable in  $\Sigma$  if there exist  $x_1 \in \mathcal{X}^{\{i\}}$  and  $x_2 \in \mathcal{X}^{\{j\}}$ , such that  $|x_1| = |x_2| = k$ ,  $x_1(h) \in \Sigma$ ,  $x_2(h) \in \Sigma$ ,  $\forall h \in [1, k]$ , and  $\mathbf{y}(x_1) = \mathbf{y}(x_2)$ .

*Remark 3.2.* Indistinguishability was defined in [23] with a different meaning. By recasting the definitions of [23] in our framework, two states  $i$  and  $j$  were said to be indistinguishable if  $\mathcal{X}_{\{i\}} = \mathcal{X}_{\{j\}}$ . In the same paper, two forward indistinguishable states as in Definition 3.1 were called *possibly indistinguishable*, while two backward indistinguishable states were called *possibly indistinguishable* with respect to a FSM associated to the given FSM  $M$ , called *reverse* FSM

The following subsets of  $\Pi$  will be instrumental in characterizing the diagnosability properties described in Definitions 2.1, 2.4, 2.5 and 2.6.

- $S^* \subset \Pi$ : set of pairs of states reachable from  $X_0$  with two indistinguishable state evolutions
- $F^* \subset \Pi$ : set of forward indistinguishable pairs of states
- $B^*(\Sigma) \subset \Sigma \subset \Pi$ : set of backward indistinguishable pairs of states that belong to a given set  $\Sigma$
- $\Lambda^* \subset (F^* \cap S^*)$ : the set of pairs  $(i, j) \in \Pi$ , with  $i \in \Omega$  and  $j \in \overline{\Omega}$  (or vice-versa  $i \in \overline{\Omega}$  and  $j \in \Omega$ ) for which there exist two indistinguishable infinite state trajectories starting from  $\{i\}$  and  $\{j\}$ , respectively, such that the latter is contained in  $\overline{\Omega}$  (or vice-versa the former is contained in  $\overline{\Omega}$ ).
- $\Gamma^* \subset B^*(S^*) \subset S^*$ : set of pairs  $(i, j) \in \Pi$ , with  $i \in \Omega$  and  $j \in \overline{\Omega}$  (or vice-versa  $i \in \overline{\Omega}$  and  $j \in \Omega$ ) for which there exist two indistinguishable finite state trajectories of arbitrary length ending in  $\{i\}$  and in  $\{j\}$ , respectively, both contained in  $S^*$ , such that the latter is contained in  $\overline{\Omega}$  (or vice-versa the former is contained in  $\overline{\Omega}$ ).

Let us give an example of the sets defined above. Because of the simplicity of the example, such sets can be determined by inspection.

**Example 3.3.** Consider the FSM depicted in Figure 5, with  $X_0 = \{1, 8\}$  and  $\Omega = \{1, 4\}$

It is easily seen that:

$$\begin{aligned}
 S^* &= \{(1, 8), (2, 5), (4, 6)\}^- \cup \Theta \\
 F^* &= \{(1, 2), (1, 5), (1, 8), (2, 5), (2, 8), (5, 8)\}^- \cup \Theta \\
 B^*(S^*) &= \{(2, 5), (4, 6)\}^- \cup (\Theta \setminus \{(1, 1)\}) \\
 \Lambda^* &= \{(1, 8)\}^- \\
 \Gamma^* &= \{(4, 6)\}^-
 \end{aligned}$$

In the following subsections, we will formally define the above sets and give algorithms for their computation. We will prove that the computation of these sets has polynomial complexity in the state cardinality  $|X|$ . In fact



the sets  $S^*$ ,  $B^*(\Sigma)$ ,  $F^*$ ,  $\Gamma^*$  and  $\Lambda^*$  are computed as fixed points of appropriate recursions, whose convergence is assured after a number of steps denoted by  $s^*$ ,  $b^*$ ,  $f^*$ ,  $g^*$  and  $l^*$ , all upper bounded by  $|X|^2$ .

### 3.1. The set $S^*$ .

**Definition 3.4.** The set  $S^*$  is the maximal set of pairs  $(i, j) \in \Pi$  such that there exist two indistinguishable state executions  $x_1 \in \mathcal{X}^{\{i\}} \cap \mathcal{X}_{X_0}$  and  $x_2 \in \mathcal{X}^{\{j\}} \cap \mathcal{X}_{X_0}$ .

The pair of states in  $S^*$  are indistinguishable in the sense of [33] and of [26], where algorithms were studied, in the framework of Mealy automata with partially observable transitions.<sup>1</sup>

In our framework, the set  $S^*$  can be computed as follows.

Define the recursion, with  $k = 1, 2, \dots$

$$(3.1) \quad \begin{aligned} S_1 &= (X_0 \times X_0) \cap \Pi \\ S_{k+1} &= \{(i, j) \in \Pi : (pre(i) \times pre(j)) \cap S_k \neq \emptyset\} \cup S_k \end{aligned}$$

**Lemma 3.5.** Consider the equation (3.1). Then,

- i) the least fixed point of the recursion, containing  $(X_0 \times X_0) \cap \Pi$ , exists, is unique and is equal to  $S^*$ ;
- ii) the recursion reaches the fixed point  $S^*$  in at most  $s^* < |X|^2$  steps.

*Proof.* The set  $\Pi$  is a fixed point of the recursion and the intersection of fixed points is a fixed point. Therefore the least fixed point containing  $(X_0 \times X_0) \cap \Pi$  exists and is unique. Let  $\widehat{S}$  denote such a fixed point. Then

$$\widehat{S} = \{(i, j) \in \Pi : (pre(i) \times pre(j)) \cap \widehat{S} \neq \emptyset\} \cup \widehat{S}$$

and hence  $\{(i, j) \in \Pi : (pre(i) \times pre(j)) \cap \widehat{S} \neq \emptyset\} \subset \widehat{S}$ . Suppose that  $S_k \subset \widehat{S}$ . Then  $S_{k+1}$  is a subset of  $\left(\{(i, j) \in \Pi : (pre(i) \times pre(j)) \cap \widehat{S} \neq \emptyset\} \cup S_k\right) \subset \widehat{S}$ . Since  $S_1 \subset \widehat{S}$ , then, by induction,  $S_k \subset \widehat{S}$ ,  $\forall k = 1, 2, \dots$ . If  $S_{k+1} = S_k$  for some  $k$  then  $S_{k+i} = S_k$ ,  $\forall i \geq 0$ , and hence  $S_k$  is a fixed point. But a finite  $k$  such that  $S_{k+1} = S_k$  exists because of the finite cardinality of  $\Pi$ . Let  $\widehat{k}$  be the minimum value of  $k$  such that  $S_{k+1} = S_k$ . It is clear that  $\widehat{k}$  is bounded by the number of not ordered pairs in  $\Pi$ . Hence  $\widehat{k} \leq \frac{|X|(|X|-1)}{2}$ . Therefore  $S_{\widehat{k}} = \widehat{S}$ . The fact that  $S^* = S_{\widehat{k}}$  comes from the maximality of  $S^*$  (see Definition 3.4). The statements i) and ii) are therefore proved.  $\square$

Let  $n_k = |S_k|$ ,  $p = |\Pi|$  and  $\nu = \max_{i \in N} |pre(i)|$ . Then at step  $k + 1$  the algorithm involves at most  $\nu^2(p - n_k)n_k$  elementary computations, where an elementary computation is: given  $(i, j) \in \Pi \setminus S_k$  and the pair  $(i', j') \in pre(i) \times pre(j)$  check whether  $(i', j') \in S_k$ . Since  $\nu^2(p - n_k)n_k \leq \nu^2|X|^4$ , then the algorithm will stop after at most  $2\nu^2|X|^4 \ln |X|$  elementary computations. Hence the spatial complexity is  $O(|X|^2)$  and the time complexity is  $O(|X|^5)$ . Similar observations on complexity hold for all the algorithms we will describe in the following sections.

### 3.2. The sets $F^*$ and $B^*(\Sigma)$ .

**Definition 3.6.** The set  $F^*$  is the maximal set of pairs  $(i, j) \in \Pi$  which are  $k$ -forward indistinguishable,  $\forall k \in \mathbb{Z}$ ,  $k \geq 1$ .

<sup>1</sup>In [33] the relation between indistinguishability and the observability notion introduced in [18] is also established.

Define the recursion, with  $k = 1, 2, \dots$ ,

$$(3.2) \quad \begin{aligned} F_1 &= \Pi \\ F_{k+1} &= \{(i, j) \in F_k : (\text{succ}(i) \times \text{succ}(j)) \cap F_k \neq \emptyset\} \end{aligned}$$

**Lemma 3.7.** *Consider equation (3.2). Then,*

- i)  $F_k$  is the set of all  $k$ -forward indistinguishable pairs;
- ii) the maximal fixed point of the recursion, contained in  $\Pi$ , is unique, nonempty and is equal to  $F^*$ ;
- iii) the recursion reaches its maximal fixed point  $F^*$  in  $f^* < |X|^2$  steps.

*Proof.* Statement i) is true by definition of  $k$ -forward indistinguishable pairs. Because of liveness assumption, the set  $\Theta$  is a fixed point of the recursion defined in equation (3.2), contained in  $\Pi$ . The union of fixed points in  $\Pi$  is a fixed point in  $\Pi$  and therefore the maximal fixed point of the recursion, contained in  $\Pi$ , is unique and nonempty. Let  $\widehat{F}$  be such fixed point. Then  $\forall (i, j) \in \widehat{F}, (\text{succ}(i) \times \text{succ}(j)) \cap \widehat{F} \neq \emptyset$ . Let us suppose that  $\widehat{F} \subset F_k$ . Then  $\widehat{F} \subset F_{k+1}$ . Since  $\widehat{F} \subset F_1$ , then, by induction,  $\widehat{F} \subset F_k, \forall k = 1, 2, \dots$ . Moreover  $F_{k+1} \subset F_k, \forall k = 1, 2, \dots$ . If  $F_{k+1} \subset F_k$  for some  $k$  then  $F_{k+i} = F_k, \forall i \geq 0$ , and hence  $F_k$  is a fixed point. But a finite  $k$  such that  $F_{k+1} = F_k$  exists because of the finite cardinality of  $\Pi$ . Let  $\widehat{k}$  be the minimum value of  $k$  such that  $F_{k+1} = F_k$ . Then  $\widehat{F} \subset F_{\widehat{k}} \subset \widehat{F}$  and hence  $F_{\widehat{k}} = \widehat{F}$ . It is clear that  $\widehat{k}$  is bounded by the number of not ordered pairs in  $\Pi$ . Hence  $\widehat{k} \leq \frac{|X|(|X|-1)}{2}$ . The fact that  $F^* = F_{\widehat{k}}$  comes from the definition of the set  $F^*$ . The statements ii) and iii) are therefore proved.  $\square$

In a similar way, given  $\Sigma \subset \Pi$ , we can introduce the following

**Definition 3.8.** The set  $B^*(\Sigma)$  is the maximal set of pairs  $(i, j) \in \Sigma$  which are  $k$ -backward indistinguishable in  $\Sigma, \forall k \in \mathbb{Z}, k \geq 1$ .

Define the recursion, with  $k = 1, 2, \dots$ ,

$$(3.3) \quad \begin{aligned} B_1(\Sigma) &= \Sigma \\ B_{k+1}(\Sigma) &= \{(i, j) \in B_k(\Sigma) : (\text{pre}(i) \times \text{pre}(j)) \cap B_k(\Sigma) \neq \emptyset\} \end{aligned}$$

**Lemma 3.9.** *Consider equation (3.3). Then,*

- i)  $B_k(\Sigma)$  is the set of all  $k$ -backward indistinguishable pairs in  $\Sigma$ ;
- ii) if  $B^*(\Sigma) \neq \emptyset$ , then the maximal fixed point of the recursion (3.3), contained in  $\Sigma$ , is unique, nonempty and is equal to  $B^*(\Sigma)$ . Otherwise  $\exists k < |X|^2$  such that  $B_k(\Sigma) = \emptyset$ ;
- iii) If  $B^*(\Sigma) \neq \emptyset$ , the recursion reaches its maximal fixed point in  $b^* < |X|^2$  steps.

*Proof.* Statement i) is true by definition of  $k$ -backward indistinguishable pairs, since  $\Sigma \subset \Pi$ . ii) Suppose that  $B^*(\Sigma) \neq \emptyset$ . Then  $B^*(\Sigma) \subset B_k(\Sigma), \forall k = 1, 2, \dots$  and is a fixed point of the recursion defined in equation (3.3). The union of fixed points in  $\Sigma$  is a fixed point and therefore the maximal fixed point of the recursion, contained in  $\Sigma$ , is nonempty and is unique. Let  $\widehat{B}$  be such fixed point. Then  $\forall (i, j) \in \widehat{B}, (\text{pre}(i) \times \text{pre}(j)) \cap \widehat{B} \neq \emptyset$ . Let us suppose that  $\widehat{B} \subset B_k(\Sigma)$ . Then  $\widehat{B} \subset B_{k+1}(\Sigma)$ . Since  $\widehat{B} \subset B_1(\Sigma)$ , then, by induction,  $\widehat{B} \subset B_k(\Sigma), \forall k = 1, 2, \dots$ . Moreover  $B_{k+1}(\Sigma) \subset B_k(\Sigma), \forall k = 1, 2, \dots$ . If  $B_{k+1}(\Sigma) \subset B_k(\Sigma)$  for some  $k$  then  $B_{k+i}(\Sigma) = B_k(\Sigma), \forall i \geq 0$ , and hence  $B_k(\Sigma)$  is a fixed point. But a finite  $k$  such that  $B_{k+1}(\Sigma) = B_k(\Sigma)$  exists because of the finite cardinality of  $\Pi$ . Let  $\widehat{k}$  be the minimum value of  $k$  such that  $B_{k+1}(\Sigma) = B_k(\Sigma)$ . Since  $\widehat{B} \subset B_{\widehat{k}}(\Sigma) \subset \widehat{B}$ , then  $B_{\widehat{k}}(\Sigma) = \widehat{B}$ . It is clear that  $\widehat{k}$  is bounded by the number of not ordered pairs in  $\Pi$ . Hence  $\widehat{k} \leq \frac{|X|(|X|-1)}{2}$ . The fact that  $B^*(\Sigma) = B_{\widehat{k}}(\Sigma)$  comes from the definition of the set  $B^*(\Sigma)$ . If  $B^*(\Sigma) = \emptyset$ , then by definition of the recursion (3.3) there exists  $k$  such that  $B_k(\Sigma) = \emptyset$ . The statements ii) and iii) are therefore proved.  $\square$

**3.3. The sets  $\Lambda^*$  and  $\Gamma^*$ .** Given  $S^*$  and  $\Omega \subset X$ , we now define the sets  $\Lambda_k$  and  $\Lambda^*$  that are subsets of  $F_k$  and  $F^*$ , i.e. the sets of forward indistinguishable pairs, for finite and infinite steps, respectively.

**Definition 3.10.**  $\Lambda_k$  is the set of pairs  $(i, j) \in S^*$ , with  $i \in \Omega$  and  $j \in \bar{\Omega}$  (or vice-versa  $i \in \bar{\Omega}$  and  $j \in \Omega$ ) for which there exist two indistinguishable executions  $x_1 \in \mathcal{X}_{\{i\}}$  and  $x_2 \in \mathcal{X}_{\{j\}}$ ,  $|x_1| = |x_2| = k$ , such that  $x_2(h) \in \bar{\Omega}$ ,  $\forall h \in [1, k]$  ( $x_1(h) \in \bar{\Omega}$ ,  $\forall h \in [1, k]$ , respectively).  $\Lambda^*$  is the set of pairs  $(i, j) \in S^*$  such that

$$\forall \bar{k} \in \mathbb{Z}, \exists k \geq \bar{k} : (i, j) \in \Lambda_k$$

The sets  $\Lambda_k$  and  $\Lambda^*$  can be computed by defining the recursion,  $k = 1, 2, \dots$

$$(3.4) \quad \begin{aligned} \Psi_1 &= (X \times \bar{\Omega}) \cap S^* \\ \Psi_{k+1} &= \{(i, j) \in \Psi_k : (\text{succ}(i) \times \text{succ}(j)) \cap \Psi_k \neq \emptyset\} \end{aligned}$$

In fact, we can prove the following:

**Lemma 3.11.** *Consider equation (3.4). Then,*

- i)  $\Lambda_k = (\Psi_k \cap (\Omega \times \bar{\Omega}))^-$ ;
- ii) If  $\Psi_k \neq \emptyset$ ,  $\forall k = 1, 2, \dots$ , the maximal fixed point  $\Psi^*$  of the recursion defined in (3.4), contained in  $X \times \bar{\Omega}$ , is nonempty and unique. Otherwise  $\exists k < |X|^2$  such that  $\Psi_k = \emptyset$  and  $\Psi^* = \emptyset$ ;
- iii) If  $\Psi^* \neq \emptyset$  the recursion defined in (3.4) reaches this maximal fixed point in  $l^* < |X|^2$  steps;
- iv)  $\Lambda^* = (\Psi^* \cap (\Omega \times \bar{\Omega}))^-$ .

*Proof.* The recursion defined in equation (3.4), up to the initialization, is identical to recursion defined in (3.2). Therefore  $\Psi_k$  is the set of  $k$ -forward indistinguishable pairs  $(i, j)$  for which there exists two indistinguishable state trajectories  $x_1 \in \mathcal{X}_{\{i\}}$  and  $x_2 \in \mathcal{X}_{\{j\}}$ , with  $|x_1| = |x_2| = k$ , such that  $x_2(h) \in \bar{\Omega}$ ,  $\forall h = 1 \dots k$ . Therefore statement i) is true by definition of  $\Lambda_k$ . By using the same arguments as in the proof of Lemma 3.7, the maximal fixed point  $\Psi^*$  of the recursion 3.4, contained in  $X \times \bar{\Omega}$  is unique. However it could be equal to the emptyset. If  $\Psi^* \neq \emptyset$ , then again by using the same arguments as in the proof of Lemma 3.7, there exists  $\hat{k} < |X|^2$  such that  $\Psi_{\hat{k}+1} = \Psi_{\hat{k}}$  and hence statements ii) and iii) hold. If  $\Psi^* = \emptyset$ , then  $\Psi_{\hat{k}} = \emptyset$ , for some  $\hat{k} < |X|^2$ , and again statements ii) and iii) hold. The last statement comes from the definition of  $\Lambda^*$ .  $\square$

It can be easily verified that:

$$(3.5) \quad \begin{aligned} \Lambda_1 &= ((\Omega \times \bar{\Omega}) \cup (\bar{\Omega} \times \Omega)) \cap S^* \\ \Lambda_{k+1} &\subset \Lambda_k \subset (F_k \cap S^*) \\ \Lambda^* &= \bigcap_{k \in \mathbb{Z}} \Lambda_k \subset (F^* \cap S^*) \end{aligned}$$

The sets  $\Gamma_k$  and  $\Gamma^*$  take into account the "backward executions" of the FSM. In fact they are subsets of  $B_k(S^*)$  and of  $B^*(S^*)$ , respectively, and are defined as follows:

**Definition 3.12.**  $\Gamma_k$  is the set of pairs  $(i, j) \in S^*$ , with  $i \in \Omega$  and  $j \in \bar{\Omega}$  (or vice-versa  $i \in \bar{\Omega}$  and  $j \in \Omega$ ) for which there exist two indistinguishable executions  $x_1 \in \mathcal{X}^{\{i\}}$  and  $x_2 \in \mathcal{X}^{\{j\}}$ ,  $|x_1| = |x_2| = k$ , such that  $(x_1(h), x_2(h)) \in S^* \cap (X \times \bar{\Omega})$ ,  $\forall h \in [1, k]$  (vice-versa  $(x_1(h), x_2(h)) \in S^* \cap (\bar{\Omega} \times X)$   $\forall h \in [1, k]$ , respectively).  $\Gamma^*$  is the set of pairs  $(i, j) \in S^*$  such that

$$\forall \bar{k} \in \mathbb{Z}, \exists k \geq \bar{k} : (i, j) \in \Gamma_k$$

Define the recursion, with  $k = 1, 2, \dots$

$$(3.6) \quad \begin{aligned} \Xi_1 &= (X \times \overline{\Omega}) \cap S^* \\ \Xi_{k+1} &= \{(i, j) \in \Xi_k : (\text{prec}(i) \times \text{prec}(j)) \cap \Xi_k \neq \emptyset\} \end{aligned}$$

**Lemma 3.13.** *Consider equation (3.6). Then,*

- i)  $\Gamma_k = (\Xi_k \cap (\Omega \times \overline{\Omega}))^-$
- ii) *If  $\Xi_k \neq \emptyset \forall k$ , then the maximal fixed point  $\Xi^*$  of the recursion, contained in  $(X \times \overline{\Omega}) \cap S^*$ , is unique and nonempty. Otherwise  $\exists k < |X|^2$  such that  $\Xi_k = \emptyset$  and  $\Xi^* = \emptyset$ .*
- iii) *If  $\Xi^* \neq \emptyset$ , the recursion reaches this maximal fixed point in  $g^* < |X|^2$  steps*
- iv)  $\Gamma^* = (\Xi^* \cap (\Omega \times \overline{\Omega}))^-$ .

*Proof.* The recursion defined in equation (3.6), up to the initialization, is identical to the recursion defined in (3.3). Therefore  $\Xi_k$  is the set of  $k$ -backward indistinguishable pairs  $(i, j)$  for which there exists two indistinguishable state trajectories  $x_1 \in \mathcal{X}^{(i)}$  and  $x_2 \in \mathcal{X}^{(j)}$ , with  $|x_1| = |x_2| = k$ , such that  $x_2(h) \in \overline{\Omega}$ ,  $\forall h = 1 \dots k$ . Therefore statement i) is true by definition of  $\Gamma_k$ . By using the same arguments as in the proof of Lemma 3.9, the maximal fixed point  $\Xi^*$  of the recursion (3.6), contained in  $(X \times \overline{\Omega}) \cap S^*$  is unique. However it could be equal to the emptyset. If  $\Xi^* \neq \emptyset$ , then again by using the same arguments as in the proof of Lemma 3.9, there exists  $\hat{k} < |X|^2$  such that  $\Xi_{\hat{k}+1} = \Xi_{\hat{k}}$  and hence statements ii) and iii) hold. If  $\Xi^* = \emptyset$ , then  $\Xi_{\hat{k}} = \emptyset$ , for some  $\hat{k} < |X|^2$ , and therefore statements ii) and iii) hold. The last statement comes from the definition of  $\Gamma^*$ .  $\square$

It can be easily verified that:

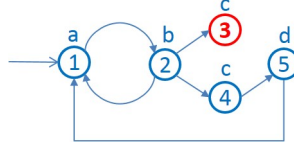
$$(3.7) \quad \begin{aligned} \Gamma_1 &= ((\Omega \times \overline{\Omega}) \cup (\Omega \times \overline{\Omega})) \cap S^* \\ \Gamma_{k+1} &\subset \Gamma_k \subset B_k(S^*) \\ \Gamma^* &= \bigcap_{k \in \mathbb{Z}} \Gamma_k \subset B^*(S^*) \subset S^* \end{aligned}$$

#### 4. MAIN RESULTS

In this section we characterize the properties introduced in Definitions 2.1, 2.4, 2.5 and 2.6. We first derive necessary and sufficient conditions for each of those properties to hold. Then, some equivalent conditions are given in terms of simple set inclusions depending on the existence of some suitable parameters. The values of these parameters allow the computation of an upper bound for the delay of the diagnosis, and of a lower bound for the uncertainty radius of the diagnosis.

Given the FSM  $M = (X, X_0, Y, H, \Delta)$ , define the FSM  $\widetilde{M} = (X, X_0, Y, H, \widetilde{\Delta})$ , where  $(i, j) \in \widetilde{\Delta}$  if and only if  $(i, j) \in \Delta$  and  $i \notin \Omega$ . Let  $\widetilde{S}^*$  be the set of pairs reachable from  $X_0$  with two indistinguishable state evolutions, computed for  $\widetilde{M}$ . Obviously  $\widetilde{S}^* \subset S^*$ .

The FSM  $\widetilde{M}$  is not alive in general. However, as pointed out in Section 3, the algorithm for the computation of  $S^*$  does not depend on the liveness assumption, so the set  $\widetilde{S}^*$  can be computed by means of the same algorithm as  $S^*$ . As an example, consider the FSM represented in Figure 2. The FSM  $\widetilde{M}$  is represented in Figure 6.

FIGURE 6. The FSM  $\widetilde{M}$ , corresponding to FSM  $M$  in Fig. 2.

The finite nonnegative values  $b^*$ ,  $\tilde{b}^*$ ,  $f^*$ ,  $g^*$  and  $l^*$  are well defined:

$$b^* = \min b : B^*(S^*) = B_b(S^*)$$

$$\tilde{b}^* = \min b : B^*(\tilde{S}^*) = B_b(\tilde{S}^*)$$

$$f^* = \min f : F^* = F_f$$

$$g^* = \min g : \Gamma^* = \Gamma_g$$

$$l^* = \min l : \Lambda^* = \Lambda_l$$

**4.1. Parametric  $\Omega$ - diagnosability.** Consider the set  $B^*(\tilde{S}^*) \cap \Lambda^*$ . On the basis of the definition of the sets given in the previous section, a pair of states  $(i, j)$  in the set  $B^*(\tilde{S}^*) \cap \Lambda^*$  is such that only one of the two states  $i$  or  $j$  belongs to  $\Omega$ . Such  $i$  and  $j$  are the ending states of a pair of arbitrarily long indistinguishable state executions of the system  $\widetilde{M}$  (which are also executions of  $M$ ) with initial states in  $X_0$ , with one of these executions which never crosses the set  $\Omega$ . Moreover,  $i$  and  $j$  are the initial states of a pair of arbitrarily long indistinguishable state executions of the system  $M$ , with one of these executions which never crosses the set  $\Omega$ . Therefore, given these executions, however long the transient and the delay are, and however loose is the required accuracy, it will not be possible to decide whether the critical set  $\Omega$  has been crossed or not. As a consequence, bearing in mind the definition of  $\widetilde{M}$  and the equivalence between parametric  $\Omega$ -diag and parametric  $\Omega$ -diag with  $T = 0$ , we can establish the following necessary and sufficient condition for an FSM to be parametrically  $\Omega$ -diag.

**Theorem 4.1.**  *$M$  is parametrically  $\Omega$ -diag if and only if*

$$(4.1) \quad B^*(\tilde{S}^*) \cap \Lambda^* = \emptyset$$

*Proof. Sufficiency:* By definition of  $\widetilde{M}$  and of  $\tilde{S}^*$ , the set

$$\{i \in \Omega : (i, j) \in B^*(\tilde{S}^*), i \neq j\}$$

describes the set of all states  $i$  in  $\Omega$ , such that for any  $k \geq \tilde{b}^*$  there exists a state execution  $x \in \mathcal{X}_{X_0}$ , with finite  $k_x \geq k$ ,  $x(k_x) = i$ , but the value of the state  $x(k_x)$  cannot be reconstructed, knowing the output evolution up to step  $k_x$ . If  $B^*(\tilde{S}^*) = \emptyset$ , then there exists  $k' \geq \tilde{b}^*$  such that any execution in  $\mathcal{X}$  is such that either  $k_x = \infty$  or  $k_x < k'$ . But  $B^*(\tilde{S}^*) = B_{\tilde{b}^*}(\tilde{S}^*)$ , and therefore  $k' = \tilde{b}^*$ . Hence the condition in Definition 2.1 is satisfied with  $T = 0$ ,  $\tau = \tilde{b}^*$  and  $\delta = 0$ . By definition of  $\Lambda^*$ , if  $\Lambda^* = \emptyset$  then given a pair  $(i, j) \in \Omega \times \overline{\Omega}$ , any state execution  $x \in \mathcal{X}_{\{j\}, \infty}$  is such that  $x(h) \in \Omega$ , for some  $h \in [1, l^*]$ . Therefore if  $\Lambda^* = \emptyset$  the condition in Definition 2.1 is satisfied with  $T = 0$ ,  $\tau = 0$ ,  $\delta = l^* - 1$ ,  $\gamma_1 = \gamma_2 = l^* - 1$ . Finally, if  $B^*(\tilde{S}^*) \cap \Lambda^* = \emptyset$ , then the condition in Definition 2.1 is satisfied with  $T = 0$ ,  $\tau = \tilde{b}^*$ ,  $\delta = l^* - 1$ ,  $\gamma_1 = \gamma_2 = \tilde{l}^* - 1$  and the proof of the sufficiency is complete. **Necessity:** By Definition 2.1  $M$  is parametrically  $\Omega$ -diag only if it is so with  $T = 0$ . Suppose that  $B^*(\tilde{S}^*) \cap \Lambda^* \neq \emptyset$ . Then since  $\Lambda^* \subset F^*$ ,  $B^*(\tilde{S}^*) \cap F^*$  is not a subset of  $\overline{\Lambda^*}$ . Hence

there exists  $(i, j) \in B^*(\tilde{S}^*) \cap F^*$  which belongs to  $\Lambda^*$ . Then, by definition of  $B^*(\tilde{S}^*)$  and of  $\Lambda^*$  it is not possible to decide about the crossing of the set  $\Omega$  with any delay. Hence  $M$  is not parametrically  $\Omega - diag$ , with  $T = 0$ . Hence it is not parametrically  $\Omega - diag$ .  $\square$

As a consequence of the result above, the following equivalent condition can be obtained

**Corollary 4.2.** *If there exist  $b \in [1, \tilde{b}^*]$ ,  $f \in [1, f^*]$  and  $l \in [1, l^*]$  such that*

$$(4.2) \quad (B_b(\tilde{S}^*) \cap F_f) \subset \overline{\Lambda_l}$$

*then  $M$  is parametrically  $\Omega - diag$  with  $T = 0$ ,  $\tau = b - 1$ ,  $\delta = \max\{f, l\} - 1$ ,  $\gamma_1 = \gamma_2 = l - 1$ . Conversely, if  $M$  is parametrically  $\Omega - diag$ , then there exist  $b \in [1, \tilde{b}^*]$ ,  $f \in [1, f^*]$  and  $l \in [1, l^*]$  such that inclusion (4.2) holds.*

*Proof.* Since  $\Lambda^* \subset (F^* \cap S^*)$ , then  $B^*(\tilde{S}^*) \cap \Lambda^* = \emptyset$  if and only if  $B^*(\tilde{S}^*) \cap \Lambda^* \cap F^* \cap S^* = \emptyset$ , which is equivalent to write  $B^*(\tilde{S}^*) \cap F^* \cap S^* \subset \overline{\Lambda^*}$ . Since  $\tilde{S}^* \subset S^*$ , then the condition 4.1 is equivalent to the inclusion

$$(B^*(\tilde{S}^*) \cap F^*) \subset \overline{\Lambda^*}$$

Moreover,  $(B^*(\tilde{S}^*) \cap F^*) \subset (B_b(\tilde{S}^*) \cap F_f)$ ,  $\forall b \in [1, \tilde{b}^*]$ ,  $\forall f \in [1, f^*]$  and  $\Lambda^* \subset \Lambda_l$ ,  $\forall l \in [1, l^*]$ . Therefore, if for some  $b \in [1, \tilde{b}^*]$ , for some  $f \in [1, f^*]$  and for some  $l \in [1, l^*]$  the inclusion 4.2 holds, then we can write

$$(B^*(\tilde{S}^*) \cap F^*) \subset (B_b(\tilde{S}^*) \cap F_f) \subset \overline{\Lambda_l} \subset \overline{\Lambda^*}$$

and hence the first statement comes from the sufficient part of Theorem 4.1. The evaluation of the parameters  $T$ ,  $\tau$ ,  $\delta$ ,  $\gamma_1$  and  $\gamma_2$  is obvious. The second statement is straightforward from the necessity part of the same Theorem 4.1.  $\square$

In the statement of the previous corollary, the parameters  $b$ ,  $f$  and  $l$  appear explicitly. Note that  $\Lambda^* \subset F^*$  but in general  $\Lambda_l$  is not a subset of  $F_f$ , for  $l \neq l^*$  or  $f \neq f^*$ . Therefore the inclusion (4.2) defines the set of all the values  $b$ ,  $f$  and  $l$  such that  $M$  is parametrically  $\Omega - diag$ . Given this set, an upper bound for the delay and a lower bound for the uncertainty radius can be evaluated. Let us explain how this can be done, in particular how the condition (4.2) allows the determination of the delay of the diagnosis of the crossing event, of the uncertainty about the time at which the event occurred and of the duration of the transient where the diagnosis is not possible or not required. This description gives also the tools for the design of the online diagnoser.

Suppose (4.2) holds for some  $b$ ,  $f$  and  $l$ . Given an infinite execution  $x$  and the output string up to current step  $k \geq b + \max\{f, l\} - 1$ , let  $\hat{x}(k) \in 2^X$  be the set of discrete states at step  $k - (\max\{f, l\} - 1)$  that are compatible with the observations up to step  $k$ . Suppose that  $k_x \geq b$ . Then at  $k = k_x + \max\{f, l\} - 1$ ,  $\hat{x}(k) \cap \Omega \neq \emptyset$ . If  $\hat{x}(k) \subset \Omega$ , then we can deduce that the set  $\Omega$  was crossed at step  $k_x = k - (\max\{f, l\} - 1)$ . Otherwise suppose that  $\hat{x}(k) = \{i, j, h\}$ , with only the state  $i$  belonging to  $\Omega$ . Then each pair  $(i, j)$ ,  $(i, h)$  and  $(j, h)$  belongs to  $(B_b(\tilde{S}^*) \cap F_f)$ , because they have not been distinguished at step  $k$ . Since the inclusion (4.2) holds, then at step  $k$  we are sure that the actual execution  $x$  of  $M$  is such that  $x(h) \in \Omega$ , for some  $h \in [k_x, k_x + l - 1]$ . Suppose that  $b > 1$  and  $k_x \leq b - 1$ . Since  $B_{k_x}(\tilde{S}^*)$  is not in general a subset of  $B_b(\tilde{S}^*)$ , then condition (4.2) does not allow the detection of the crossing event, based on the information available at step  $k_x + \max\{f, l\} - 1$ . Hence detection of the first crossing event occurs with a maximum delay  $\delta = \max\{f, l\} - 1$ , with uncertainty  $\gamma = l - 1$  and with  $\tau = b - 1$ . Therefore the system is parametrically diagnosable with  $T = 0$ ,  $\delta = \max\{f, l\} - 1$ ,  $\gamma = l - 1$  and  $\tau = b - 1$ . Finally, since  $B_1(\tilde{S}^*) = \tilde{S}^*$ ,  $F_1 = \Pi$ ,  $\Lambda_1 = ((\Omega \times \overline{\Omega}) \cup (\overline{\Omega} \times \Omega))$ , then if (4.2)

holds in the very special case of  $b = f = l = 1$ , then  $\tilde{S}^* \subset ((\Omega \times \Omega) \cup (\overline{\Omega} \times \overline{\Omega}))$ , and detection occurs with a maximum delay  $\delta = 0$ , with uncertainty  $\gamma = 0$  and with  $\tau = 0$ .

**4.2.  $\Omega$ –diagnosability.** Consider now  $\Omega$ –diagnosability as defined in Definition 2.4.

Consider the set  $\tilde{S}^* \cap \Lambda^*$ . By similar reasoning as in the previous subsection, the set  $\tilde{S}^* \cap \Lambda^*$  is the set of pairs  $(i, j)$ , where only one of the two states  $i$  or  $j$  belongs to  $\Omega$ , which are the ending states of a pair of indistinguishable state executions of the system  $\tilde{M}$ , with initial state in  $X_0$ , such that one of these executions never crosses the set  $\Omega$ , and are the initial states of a pair of arbitrarily long indistinguishable state executions of the system  $M$ , such that one of them never crosses  $\Omega$ . Therefore, recalling the definition of the system  $\tilde{M}$ , we can prove the following:

**Theorem 4.3.**  *$M$  is  $\Omega$  – diag if and only if*

$$(4.3) \quad \tilde{S}^* \cap \Lambda^* = \emptyset$$

*Proof. Sufficiency:* Setting  $b = 1$  in condition (4.2),  $B_1(\tilde{S}^*) = \tilde{S}^*$  and we obtain condition (4.3). Hence  $\tau = 0$  and  $M$  is  $\Omega$  – diag. *Necessity:* if  $\tilde{S}^* \cap \Lambda^* \neq \emptyset$  then for any  $f, l \in \mathbb{Z}$ , and since  $\Lambda^* \subset F^*$  there exists  $(i, j) \in \tilde{S}^* \cap F^*$ , such that  $(i, j) \in \Lambda_l$ . Then there exists  $x \in \mathcal{X}$  such that  $x(k) = i$  (or  $j$ ), and the pair  $(i, j)$  cannot be distinguished at step  $k + f$  from  $\mathbf{y}(x|_{[1, k+f]})$ ,  $\forall f \in \mathbb{Z}$ . Since  $(i, j) \in \Lambda^*$  there exists a pair  $(x_1, x_2)$  of infinite indistinguishable evolutions starting from  $(i, j)$ , with the property that only one of them crosses the set  $\Omega$ . Therefore there does not exist  $\delta$  such that at step  $k + \delta$  it is possible to decide if a crossing event occurred in the interval  $[1, k + \delta]$ . Hence the given condition is necessary.  $\square$

Condition (4.3) implies diagnosability as defined in [25]. The proof of the necessity in Theorem 4.3 above shows that condition (4.3) is necessary also for the property of [25] to hold. Hence, the diagnosability property of Definition 2.4 and the one defined in [25] are equivalent.

As in the previous subsection, we obtain the following equivalent condition expressed in terms of the parameters for which  $\Omega$ –diagnosability holds.

**Corollary 4.4.** *The FSM  $M$  is  $\Omega$  – diag with delay  $\delta$  and uncertainty radius  $\gamma$  if*

$$(4.4) \quad (\tilde{S}^* \cap F_f) \subset \overline{\Lambda}_l$$

where  $f \leq \delta + 1$ ,  $l \leq \delta + 1$  and  $l \leq \gamma + 1$ . Conversely, if  $M$  is  $\Omega$  – diag, then there exist  $f \in [1, f^* - 1]$  and  $l \in [1, l^* - 1]$  such that inclusion (4.4) holds.

*Proof.* Straightforward consequence of Theorem 4.3.  $\square$

Condition (4.4) gives the tools for the computation of the delay between the occurrence of the critical event and its detection. More precisely, let us explain how the condition (4.4) allows the determination of the delay of the diagnosis of the crossing event and the uncertainty about the time at which the event occurred, and how the online detection can be done.

Suppose (4.4) holds for some  $f$  and  $l$ . Let  $k'$  be the first  $k \geq \max\{f, l\}$  such that  $\hat{x}(k) \cap \Omega \neq \emptyset$ . If  $\hat{x}(k') \subset \Omega$ , then we can deduce that the set  $\Omega$  was crossed for the first time at step  $k' - (\max\{f, l\} - 1)$ . Otherwise suppose that  $\hat{x}(k') = \{i, j, h\}$ , with only the state  $i$  belonging to  $\Omega$ . Then each pair  $(i, j)$ ,  $(i, h)$  and  $(j, h)$  belongs to  $\tilde{S}^* \cap F_f$ . Since the inclusion (4.4) holds, then any pair of indistinguishable state evolution of  $M$  starting from  $\tilde{S}^* \cap F_f$  is such that both evolutions in the pair cross the set  $\Omega$  within at most  $l$  steps. Therefore at step  $k'$  we are sure that the actual evolution of  $M$  is such that  $x(h) \in \Omega$ , for some  $h \in [k' - (\max\{f, l\} - 1), k' - \max\{f, l\} + l]$ . Hence detection occurs with a maximum delay  $\delta = \max\{f, l\} - 1$ , and with uncertainty  $\gamma = l - 1$ .

The next result characterizes  $\Omega$ –initial state observability (see Definition 2.4), a special case of  $\Omega$ –diagnosability.

**Corollary 4.5.**  *$M$  is  $\Omega$ -initial state observable if and only if*

$$(4.5) \quad (X_0 \cap F^*) \subset (\Omega \times \Omega) \cup (\overline{\Omega} \times \overline{\Omega})$$

*Proof. Sufficiency:* If condition (4.4) holds with  $l = 1$ , then  $\gamma_1 = \gamma_2 = 0$  and  $M$  is  $\Omega$ -initial state observable. Since  $\overline{\Lambda}_1 = (\Omega \times \Omega) \cup (\overline{\Omega} \times \overline{\Omega})$  and  $\tilde{S}^* = X_0$ , condition (4.4) boils down to inclusion 4.5 and the sufficiency follows. **Necessity:** obvious.  $\square$

**4.3. Eventual and critical  $\Omega$ -diagnosability.** Consider the eventual  $\Omega$ -diagnosability property as defined in Definition 2.5.

For simplicity, in this sub-section, the sets  $B^*(S^*)$  and  $B_k(S^*)$  will be denoted by  $B^*$  and  $B_k$ .

A pair  $(i, j)$  in the set  $\Gamma^* \cap \Lambda^*$  is such that only one state of the pair belongs to  $\Omega$ . The states  $i$  and  $j$  are the ending states of a pair of arbitrarily long indistinguishable state executions of the system  $M$ , with initial state in  $X_0$ , such that one of these executions never crosses the set  $\Omega$ , and are the initial states of a pair of arbitrarily long indistinguishable state executions of the same system  $M$ , such that one of these executions never crosses the set  $\Omega$ . Therefore we can prove the following:

**Theorem 4.6.** *The FSM  $M$  is eventually  $\Omega$ -diag if and only if*

$$(4.6) \quad \Gamma^* \cap \Lambda^* = \emptyset$$

*Proof. Sufficiency:* Let  $\tau = g^*$ . By definition of  $\Gamma^*$ , if  $\Gamma^* = \emptyset$  then if for some  $k \geq \tau + 1$  the execution  $x \in \mathcal{X}_{X_0}$  is such that  $x(k) \in \Omega$ , then any  $x' \in \mathbf{y}^{-1}(\mathbf{y}(x|_{[1,k]}))$  is such that  $x'(h) \in \Omega$ , for some  $h \in [k - (g^* - 1), k]$ . Therefore condition in Definition 2.5 is satisfied with parameters  $\tau = g^*$ ,  $\gamma = g^*$  and  $\delta = g^*$ . By definition of  $\Lambda^*$ , if  $\Lambda^* = \emptyset$  then given a pair  $(i, j) \in \Omega \times \overline{\Omega}$ , any pair of indistinguishable state executions  $x'$  and  $x''$  starting from  $(i, j)$ , respectively, are such that  $x''(h) \in \Omega$ , for some  $h \in [1, l^*]$ . Therefore,  $\Lambda^* = \emptyset$  implies that, if for some  $k \geq \tau + 1$  the execution  $x \in \mathcal{X}_{X_0}$  is such that  $x(k) \in \Omega$ , then any  $x' \in \mathbf{y}^{-1}(\mathbf{y}(x|_{[1, k + \max\{f^*, l^*\} - 1]}))$  is such that  $x'(h) \in \Omega$ , for some  $h \in [k, k + (l^* - 1)]$ . Therefore condition in Definition 2.5 is satisfied with parameters  $\tau = g^*$ ,  $\gamma = l^*$  and  $\delta = l^* - 1$ . Finally, it is straightforward to check that if  $\Gamma^* \cap \Lambda^* = \emptyset$  then if for some  $k \geq \tau + 1$   $x \in \mathcal{X}_{X_0}$  is such that  $x(k) \in \Omega$ , then any  $x' \in \mathbf{y}^{-1}(\mathbf{y}(x|_{[1, k + \max\{f^*, l^*\} - 1]}))$  is such that  $x'(h) \in \Omega$ , for some  $h \in [k - (g^* - 1), k + (l^* - 1)]$ . Therefore condition in Definition 2.5 is satisfied with parameters  $\tau = g^*$ ,  $\gamma = \max\{g^*, l^*\} - 1$  and  $\delta = l^* - 1$ .

**Necessity:** Suppose that  $\Gamma^* \cap \Lambda^* \neq \emptyset$ . Then there exists  $(i, j) \in B^* \cap F^*$  such that  $(i, j) \in \Gamma^* \cap \Lambda^*$ . Therefore  $(i, j) \in ((\Omega \times \overline{\Omega}) \cup (\overline{\Omega} \times \Omega))$ . Therefore  $(i, j)$  cannot be in general distinguished and there exists two indistinguishable infinite and left unbounded trajectories crossing  $i$  and  $j$ , but only one of them crosses the set  $\Omega$ . Therefore  $M$  is not eventually  $\Omega$ -diag and the condition (4.7) is necessary.  $\square$

The following equivalent characterization of eventual  $\Omega$ -diagnosability is obtained:

**Corollary 4.7.** *If there exist  $b \in [1, b^*]$ ,  $f \in [1, f^*]$ ,  $g \in [1, g^*]$  and  $l \in [1, l^*]$  such that*

$$(4.7) \quad (B_b \cap F_f) \subset (\overline{\Gamma_g} \cap \overline{\Lambda_l})$$

*then  $M$  is eventually  $\Omega$ -diag with  $\tau = \max\{b, g\} - 1$ ,  $\delta = \max\{f, l\} - 1$ ,  $\gamma_1 = g - 1$ ,  $\gamma_2 = l - 1$ . Conversely, if  $M$  is eventually  $\Omega$ -diag, then there exist  $b \in [1, b^*]$ ,  $f \in [1, f^*]$ ,  $g \in [1, g^*]$  and  $l \in [1, l^*]$  such that inclusion (4.7) holds.*

*Proof.* Since  $\Gamma_{g^*} = \Gamma^* \subset B^* = B_{b^*}$ ,  $\Lambda_{l^*} = \Lambda^* \subset F^* = F_{f^*}$ , then  $\Gamma^* \cap \Lambda^* = \emptyset$  can be rewritten as  $B_{b^*} \cap F_{f^*} \cap \Gamma_{g^*} \cap \Lambda_{l^*} = \emptyset$ . This last condition is equivalent to  $(B_{b^*} \cap F_{f^*}) \subset (\overline{\Gamma_{g^*} \cap \Lambda_{l^*}})$ . For  $b \in [1, b^*]$ ,  $f \in [1, f^*]$ ,  $g \in [1, g^*]$  and  $l \in [1, l^*]$ , if  $(B_b \cap F_f) \subset (\overline{\Gamma_g} \cap \overline{\Lambda_l})$  we can write

$$(B_{b^*} \cap F_{f^*}) \subset (B_b \cap F_f) \subset (\overline{\Gamma_g} \cap \overline{\Lambda_l}) \subset (\overline{\Gamma_{g^*} \cap \Lambda_{l^*}})$$



Therefore the proof of the sufficiency follows from the proof of Theorem 4.6. The estimation of the parameters  $\tau$ ,  $\delta$ ,  $\gamma_1$  and  $\gamma_2$ , given the parameters  $b$ ,  $f$ ,  $g$  and  $l$  is obvious. Let us consider the last statement, and suppose that it is false, i.e.  $M$  is eventually  $\Omega - diag$  but for any choice of the parameters in the given interval the inclusion (4.7) is not satisfied. By setting  $b = b^*$ ,  $f = f^*$ ,  $g = g^*$  and  $l = l^*$  we obtain that  $\Gamma^* \cap \Lambda^* \neq \emptyset$  and hence by Theorem 4.6 it is not possible that  $M$  is eventually  $\Omega - diag$ .  $\square$

We now show how the condition (4.7) allows the determination of the delay of the diagnosis of the crossing event, of the uncertainty about the time at which the event occurred and of the duration of the transient where the diagnosis is not possible or not required.

Suppose (4.7) holds for some  $b$ ,  $f$ ,  $g$  and  $l$ . Let  $k'$  be any  $k \geq \max\{b, g\} + \max\{f, l\} - 1$  such that  $\hat{x}(k) \cap \Omega \neq \emptyset$ . If  $\hat{x}(k') \subset \Omega$ , then we can deduce that the set  $\Omega$  was crossed at step  $k'' = k' - (\max\{f, l\} - 1)$ . Otherwise suppose that  $\hat{x}(k') = \{i, j, h\}$ , with only the state  $i$  belonging to  $\Omega$ . Then each pair  $(i, j)$ ,  $(i, h)$  and  $(j, h)$  belongs to  $B_b \cap F_f$ . Since the inclusion (4.7) holds, then each pair of state evolutions  $x_1$  and  $x_2$ , compatible with the observations up to step  $k$ , and such that  $x_1(k'') = i$  and  $x_2(k'') = j$  has the property that both evolutions crossed the set  $\Omega$  in the interval  $[k'' - g + 1, k'']$ , if  $(i, j) \in \bar{\Gamma}_g$ , or in the interval  $[k'', k'' + l - 1]$ , if  $(i, j) \in \bar{\Lambda}_l$ . Therefore at step  $k'$  the actual evolution of  $M$  is such that  $x(h) \in \Omega$ , for some  $h \in [k'' - (g - 1), k' + l - 1]$ . Hence detection occurs with a maximum delay  $\delta = \max\{f, l\} - 1$ , with uncertainty  $\gamma = \max\{g, l\} - 1$  and with  $\tau = \max\{b, g\} - 1$ . Since  $B_1 = S^*$ ,  $F_1 = \Pi$ ,  $\Gamma_1 = \Lambda_1 = ((\Omega \times \bar{\Omega}) \cup (\bar{\Omega} \times \Omega))$ , then if (4.7) holds in the very special case of  $b = g = f = l = 1$ , then  $S^* \subset ((\Omega \times \Omega) \cup (\bar{\Omega} \times \bar{\Omega}))$ , and detection occurs with a maximum delay  $\delta = 0$ , with uncertainty  $\gamma = 0$  and with  $\tau = 0$ .

As a consequence of Theorem 4.6, we also obtain the following characterizations of diagnosability in two interesting special cases. The first one requires no delay in the detection (Case  $\delta = 0$ ).

**Corollary 4.8.** (Case  $\delta = 0$ )  $M$  is eventually  $\Omega - diag$  with  $\delta = 0$  if and only if

$$(4.8) \quad B^* \subset ((\Omega \times \Omega) \cup (\bar{\Omega} \times \bar{\Omega}))$$

*Proof. Sufficiency:* if we set  $f = 1$  and  $l = 1$ , then  $\delta = 0$ . Since  $F_1 = \Pi$ ,  $B^* \subset S^* \subset \Pi$  and  $\Gamma_1 = \Lambda_1 = ((\Omega \times \bar{\Omega}) \cup (\bar{\Omega} \times \Omega))$ , then condition 4.7 with  $b = b^*$  and  $g = 1$  becomes

$$B^* \subset ((\Omega \times \Omega) \cup (\bar{\Omega} \times \bar{\Omega}))$$

and hence  $M$  is eventually  $\Omega - diag$  with  $\delta = 0$ . **Necessity:** suppose that there exists  $(i, j) \in B^*$  such that  $(i, j) \in ((\Omega \times \Omega) \cup (\bar{\Omega} \times \bar{\Omega})) = ((\Omega \times \bar{\Omega}) \cup (\bar{\Omega} \times \Omega))$ . Hence for any  $k$  such that  $x(k) = i \in \Omega$ , it is not possible to decide at step  $k$  if  $x(k) \in \Omega$  or not. Hence  $M$  is not eventually  $\Omega - diag$  with  $\delta = 0$ .  $\square$

The second special case requires the exact detection of the step at which the crossing event occurred (Case  $\gamma = 0$ ).

**Corollary 4.9.** (Case  $\gamma = 0$ )  $M$  is eventually  $\Omega - diag$  with  $\gamma = 0$  if and only if condition 4.7 holds with  $g = 1$  and  $l = 1$ , i.e. there exist  $b$  and  $f$  such that

$$(4.9) \quad (B_b \cap F_f) \subset (\Omega \times \Omega) \cup (\bar{\Omega} \times \bar{\Omega})$$

*Proof.* Sufficiency is straightforward from Corollary 4.7. **Necessity:** If  $B^* = \emptyset$  then  $M$  is eventually  $\Omega - diag$  with  $\gamma = 0$  and condition (4.9) holds with  $b = b^*$ . Otherwise, suppose that for any  $b$  and  $f$  there exists  $(i, j) \in (B_b \cap F_f)$ , belonging to  $((\Omega \times \Omega) \cup (\bar{\Omega} \times \bar{\Omega})) = ((\Omega \times \bar{\Omega}) \cup (\bar{\Omega} \times \Omega))$ . Therefore there exists  $(i, j) \in B^* \cap F^*$  such that  $(i, j) \in ((\Omega \times \bar{\Omega}) \cup (\bar{\Omega} \times \Omega))$ . Hence for any  $\tau$  and for any  $\delta$  there exists an execution such that whenever  $x(k) = i$ ,  $k \geq \tau + 1$ , it is not possible to deduce from the output whether  $x(k) \in \Omega$ . Hence  $M$  is not eventually  $\Omega - diag$  with  $\gamma = 0$ .  $\square$

Finally, we characterize the property in Definition 2.6. By Proposition 2.7, a characterization of critical  $\Omega$ -diagnosability is obtained as simple consequence of Theorems 4.3 and 4.6:

**Corollary 4.10.** *M is critically  $\Omega - diag$  if and only if*

$$\begin{aligned}\tilde{S}^* \cap \Lambda^* &= \emptyset \\ \text{and} \\ \Gamma^* \cap \Lambda^* &= \emptyset\end{aligned}$$

*Proof.* Straightforward, from Proposition 2.7 and equations (4.3) and (4.6).  $\square$

The value  $\max\{b, g\} - 1$  in the statement of Corollary 4.7 is not in general the minimum value of  $\tau$  such that  $M$  is eventually  $\Omega - diag$  (see the next Example 5.3). Hence critical  $\Omega - diag$  cannot be deduced by setting  $b = g = 1$  in condition (4.7).

The next proposition characterizes critical  $\Omega$ -observability.

**Proposition 4.11.** *(Case  $\delta = 0$  and  $\tau = 0$ ) M is critically  $\Omega - obs$  if and only if*

$$(4.10) \quad S^* \subset (\Omega \times \Omega) \cup (\overline{\Omega} \times \overline{\Omega})$$

*Proof. Sufficiency:* Since  $B^* \subset S^*$  then by Corollary 4.8  $M$  is eventually  $\Omega - diag$  with  $\delta = 0$ . Since  $F_f \subset S^*$ , then by Corollary 4.10  $M$  is eventually  $\Omega - diag$  with  $\tau = 0$ . **Necessity:** By Corollary 4.8, it is necessary that  $B^* \subset ((\Omega \times \Omega) \cup (\overline{\Omega} \times \overline{\Omega}))$ . Suppose there exists  $(i, j) \in S^*$ , such that  $(i, j) \notin B^*$  and  $(i, j) \in ((\Omega \times \Omega) \cup (\overline{\Omega} \times \overline{\Omega})) = ((\Omega \times \overline{\Omega}) \cup (\overline{\Omega} \times \Omega))$ . Then there exists  $k$  such that  $x(k) = i \in \Omega$ , and it is not possible to decide at step  $k$  if  $x(k) \in \Omega$  or not. Hence  $M$  is not eventually  $\Omega - diag$  with  $\tau = 0$ .  $\square$

## 5. EXAMPLES

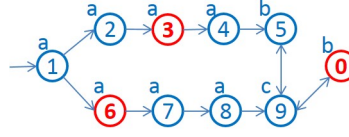
Recall that for a set  $Y \subset X$ ,  $Y^-$  denotes the symmetric closure of  $Y$ .

**Example 5.1.** ( $M$  is not parametrically  $\Omega - diag$ ) Consider the FSM represented in Figure 2. Let  $X_0 = \{1\}$  and  $\Omega = \{3\}$ . Since  $B^* \left( \tilde{S}^* \right) = \{(3, 4)\}^- \cup \Theta$  (see Figure 6) and  $\Lambda^* = \{(3, 4)\}^-$ , then  $B^* \left( \tilde{S}^* \right) \cap \Lambda^* = \{(3, 4)\}^-$  and hence by Theorem 4.1  $M$  is not parametrically  $\Omega - diag$ .

**Example 5.2.** ( $M$  is eventually  $\Omega - diag$  but not  $\Omega - diag$ ) Consider the FSM defined in Example 2.9 and depicted in Figure 3. Let  $X_0 = X$ .

$$\begin{aligned}\Pi &= \{(1, 3), (1, 5), (3, 5), (2, 4)\}^- \cup \Theta \\ S^* &= \Pi \\ B^* &= \{(1, 3)\}^- \cup \Theta, b^* = 2 \\ F^* &= \{(3, 5)\}^- \cup \Theta, f^* = 2 \\ \Gamma^* &= \{(1, 3)\}^-, g^* = 2 \\ \Lambda^* &= \{(3, 5)\}^-, l^* = 2\end{aligned}$$

Since  $\Gamma^* \cap \Lambda^* = \emptyset$ ,  $M$  is eventually  $\Omega - diag$  with  $\delta = 1$ ,  $\tau = 1$ ,  $\gamma_1 = \gamma_2 = 1$ . Moreover,  $\tilde{S}^* = \Pi$ ,  $\tilde{S}^* \cap \Lambda^* \neq \emptyset$ , and hence  $M$  is not  $\Omega - diag$ . Corollary 4.7 allows a better estimation of the parameters. In fact  $B^* \cap F^* = \Theta$  which is not a subset of  $\Gamma_1 \cap \Lambda_1$ . Therefore  $M$  is eventually  $\Omega - diag$  with  $\delta = 1$ ,  $\tau = 1$ ,  $\gamma_1 = \gamma_2 = 0$ .

FIGURE 7. FSM  $M$  (Example 5.4).

**Example 5.3.** ( $M$  is eventually  $\Omega$ -diag or critically  $\Omega$ -diag, depending on  $X_0$ ) Consider the FSM defined in Example 2.10 and represented in Figure 4. If  $X_0 = X$  then

$$\begin{aligned}\Pi &= \{(1, 2), (1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5), (3, 4), (3, 5), (4, 5), (6, 7)\}^- \cup \Theta \\ S^* &= \Pi \\ B^* = F^* &= \{(2, 4), (3, 5)\}^- \cup \Theta \\ \Gamma^* &= \{(2, 4)\}^- \\ \Lambda^* &= \{(3, 5)\}^-\end{aligned}$$

Therefore  $(\Gamma^* \cap \Lambda^*) = \emptyset$  and by Theorem 4.6  $M$  is eventually  $\Omega$ -diag. Moreover  $f^* = b^* = 3$  and  $g^* = l^* = 2$ . Hence  $M$  is eventually  $\Omega$ -diag with  $\delta = \max\{f^*, l^*\} - 1 = 2$ ,  $\tau = \max\{b^*, g^*\} - 1 = 2$ ,  $\gamma_1 = g^* - 1 = 1$ ,  $\gamma_2 = l^* - 1 = 1$ .

Since  $\tilde{S}^* = S^* = \Pi$  and  $\tilde{S}^* \cap F^*$  is not a subset of  $\overline{\Lambda^*}$ , then  $M$  is not  $\Omega$ -diag, and hence it is not critically  $\Omega$ -diag.

Suppose  $X_0 = \{1\}$ . Then

$$\begin{aligned}S^* &= \{(2, 4), (3, 5)\}^- \cup \Theta \\ B_1 = B^* &= S^* \\ F_1 = F^* &= S^* \\ \Gamma_1 = \Lambda_1 &= \{(1, 3), (1, 4), (2, 3), (2, 4), (3, 5), (4, 5)\}^- \\ \Gamma^* &= \{(2, 4)\}^- \\ \Lambda^* &= \{(3, 5)\}^- \\ \tilde{S}^* &= \{(2, 4)\}\end{aligned}$$

Since  $B_1 \cap F^* = \{(2, 4), (3, 5)\}$  and  $\Gamma_1 \cap \Lambda^* = \{(3, 5)\}$  then  $(B_1 \cap F^*)$  is not a subset of  $\overline{\Gamma_1 \cap \Lambda^*}$ . Therefore there not exist values of  $l$  and  $f$  such that the condition

$$(B_b \cap F_f) \subset \overline{\Gamma_g \cap \Lambda_l}$$

in Corollary 4.7 is satisfied for  $b = 1$  and  $g = 1$ . Hence  $\min(\max\{b, g\} - 1) > 0$ . Nevertheless,  $M$  is critically  $\Omega$ -diag. In fact  $(\Gamma^* \cap \Lambda^*) = \emptyset$  and hence by Theorem 4.6  $M$  is eventually  $\Omega$ -diag. Moreover,  $\tilde{S}^* \cap \Lambda^* = \emptyset$  and hence by Theorem 4.3  $M$  is  $\Omega$ -diag, and therefore by Proposition 2.7 it is critically  $\Omega$ -diag, and therefore it is eventually  $\Omega$ -diag with  $\tau = 0$ .

**Example 5.4.** ( $M$  is  $\Omega - diag$  but not eventually  $\Omega - diag$ ) Consider the FSM  $M$  depicted in Figure 4.4. Let  $X_0 = \{1\}$  and  $\Omega = \{3, 6, 0\}$

$$\begin{aligned}
S^* &= \{(2, 6), (3, 7), (4, 8), (0, 5)\}^- \cup \Theta \\
\tilde{S}^* &= \{(2, 6)\}^- \cup \{(1, 1), (2, 2), (3, 3), (6, 6)\} \\
B^* &= \{(0, 5)\}^- \\
F_1 &= \Pi \\
F_2 &= \{(2, 6), (2, 3), (6, 7), (0, 5)\}^- \cup \Theta \\
F_3 &= \{(2, 6), (0, 5)\}^- \\
F^* = F_4 &= \{(0, 5)\}^- \cup \Theta, f^* = 4 \\
\Lambda_1 &= \{(2, 6), (3, 7), (0, 5)\}^- \\
\Lambda^* = \Lambda_2 &= \{(0, 5)\}^- \\
\Gamma^* &= \{(0, 5)\}^-
\end{aligned}$$

This FSM is not eventually  $\Omega - diag$ , since  $\Gamma^* \cap \Lambda^* \neq \emptyset$ . It is  $\Omega - diag$ . In fact by Theorem 4.3  $(\tilde{S}^* \cap F^*) = \{(1, 1), (2, 2), (3, 3), (6, 6)\} \subset \overline{\Lambda^*}$  and hence  $M$  is  $\Omega - diag$  with  $\delta = 2$  and  $\gamma_1 = \gamma_2 = 2$ . Since  $\tilde{S}^* \cap F_2 \subset \overline{\Lambda_2}$ , then by Corollary 4.4, we can refine our estimations. In fact  $M$  is  $\Omega - diag$  with  $\delta = 1$  and  $\gamma_1 = \gamma_2 = 1$ . Moreover  $(\tilde{S}^* \cap F^*) \subset \overline{\Lambda_1}$ , and hence  $M$  is  $\Omega - diag$  with  $\delta = 3$  and  $\gamma_1 = \gamma_2 = 0$ .

## 6. APPENDIX: CASE $\epsilon \in Y$

Given the FSM  $M$ , we propose an algorithm for deriving an FSM  $\widehat{M}$  having no silent state such that the parametric diagnosability property can be checked on either FSMs equivalently. The algorithm in [7] can be retrieved from the one we are going to describe by setting  $\Omega = \emptyset$ .

Given  $M = (X, X_0, Y, H, \Delta)$ , a state  $q$  is called silent if  $H(q) = \epsilon$ . Let  $X_\epsilon$  be the set of silent states. Suppose that any cycle has at least a state  $q$  with  $H(q) \neq \epsilon$ . Suppose moreover that there is no silent state in  $X_0$  and that a state belongs to  $X_0$  if and only if it has no predecessors. We will say that a silent state  $q \in X$  is reached from  $w \in X$  with a silent execution if there exists a state execution  $x \in \mathcal{X}^*$  such that  $x(1) = w$ ,  $x(|x|) = q$  and  $\mathbf{y}(x) = H(w)$ . The symbol  $\Omega$  denotes the critical set.

The FSM  $\widehat{M} = (\widehat{X}, \widehat{X}_0, Y, \widehat{H}, \widehat{\Delta})$  is constructed as described in the following algorithm (high level description), where, when a state is removed from the state space, the transitions to and from that state are also be removed, although this is not explicitly said for the sake of simplicity.

### Algorithm 1.

**STEP 0:** Split any  $q \in X_\epsilon$  with silent and nonsilent successors into two states,  $q'$  and  $q''$ , one with only silent successors, and the other one with only nonsilent successors. The set of predecessors of  $q'$  and  $q''$  is the same as those of  $q$ . Update  $M$  accordingly. If  $q \in \Omega$ , then the set  $\Omega$  is updated by replacing  $q$  with  $q'$  and  $q''$ .

**INITIALIZE:**  $\widehat{M} = M$ . Let  $X_F \subset X \setminus X_\epsilon$  be the set of non silent states with a silent successor. Let  $X_L \subset X_\epsilon$  be the set of silent states with no silent successor.

**STEP 1:** Split any  $q \in X_L$  into  $2 * |X_F|$  states: i.e. in  $\widehat{X}$  the set  $X_L$  is substituted by the set  $\{q_w, q \in X_L, w \in X_F\} \cup \{(q_w, 1), q \in X_L, w \in X_F\}$ , where  $q_w$  is a short notation for the pair  $(q, w)$ . Therefore

$$\widehat{X} = (X \setminus X_L) \bigcup \{q_w, q \in X_L, w \in X_F\} \bigcup \{(q_w, 1), q \in X_L, w \in X_F\}$$

Moreover  $\widehat{H}(q_w) = \widehat{H}((q_w, 1)) = H(w)$ ,  $\forall q \in X_L, \forall w \in X_F$ . The symbol "1" appearing in  $(q_w, 1)$  is just a flag, whose meaning will be clarified in the description of STEP 3.

**STEP 2:** FOR  $q \in X_L$  DO

FOR  $w \in X_F$  DO

IF  $q$  is reached from  $w$  with a silent execution of  $M$ , and none of the states in this execution belongs to the set  $\Omega$ , then  $q_w \in \widehat{X}$ . If  $w \in X_0$  then  $q_w \in \widehat{X}_0$ .

OTHERWISE remove  $q_w$  from the state space  $\widehat{X}$ .

END

END

**STEP 3:** FOR  $q \in X_L$  DO

FOR  $w \in X_F$  DO

IF  $q$  is reached from  $w$  with a silent execution of  $M$ , and some of the states in this execution belong to the set  $\Omega$ , then  $(q_w, 1) \in \widehat{X}$ . If  $w \in X_0$  then  $(q_w, 1) \in \widehat{X}_0$ .

OTHERWISE remove  $(q_w, 1)$  from the state space  $\widehat{X}$ .

**STEP 4:** FOR  $q_w \in \widehat{X}$ ,  $\widehat{\Delta}$  is updated in such a way that

$$succ_{\widehat{M}}(q_w) = succ(q) \cup \{i_j \in \widehat{X} : j \in succ(q)\}$$

and

$$pre_{\widehat{M}}(q_w) = (pre(w) \cap (X \setminus X_\epsilon)) \cup \{i_j \in \widehat{X} : i \in pre(w) \cap X_\epsilon\}$$

where, to avoid ambiguities,  $succ_{\widehat{M}}$  and  $pre_{\widehat{M}}$  denote the operators  $succ$  and  $pre$  computed for the FSM  $\widehat{M}$ . If  $w \in succ(q)$  then  $(q_w, q_w) \in \widehat{\Delta}$ . A similar construction has to be done for  $(q_w, 1) \in \widehat{X}$ .

**STEP 5:** Remove all silent states and all sink states (i.e. states with no successors) from the state space  $\widehat{X}$ .

Define the set  $\widehat{\Omega}$  as  $(\Omega \cup \{(q_w, 1), q \in X_L, w \in X_F\}) \cap \widehat{X}$ .

Given  $q \in X_L$  and  $w \in X_F$ , the test in STEP 2 ( $q$  is reached from  $w$  with a silent execution, and none of the states in this execution belongs to the set  $\Omega$ ) can be done with the procedure described in (6.1), where  $\lambda$  is the maximal length of a silent string (recall that there are no silent cycles in  $M$ )

$$(6.1) \quad \begin{aligned} & C(0) = \{q\}, k = 0 \\ & \text{WHILE } (k < \lambda) \wedge (w \notin C(k)) \\ & \text{DO } k = k + 1; C(k) = \bigcup_{z \in (C(k-1)) \cap (X_\epsilon \setminus \Omega)} pre\{z\} \\ & \text{END} \end{aligned}$$

**Proposition 6.1.** *Given  $M$ , a state  $q \in X_\epsilon \setminus \Omega$  is reached from  $w \in X \setminus (X_\epsilon \cup \Omega)$  with a silent execution, and none of the states in this execution belongs to the set  $\Omega$ , if and only if the exit condition of the cycle defined in (6.1) is  $w \in C(\bar{k})$ ,  $1 \leq \bar{k} \leq \lambda$ .*

The proof of the above Proposition is obvious and hence can be omitted.

We now describe how the test in STEP 3 ( $q$  is reached from  $w$  with a silent execution, and some of the states in this execution belong to the set  $\Omega$ ) can be performed. The procedure described in (6.2) is instrumental in computing the set  $\left( \bigcup_{k=1 \dots g} V(k) \right)$ , for a given  $g \in [2, \lambda]$ , required in the statement of the next Proposition 6.2

$$\begin{aligned}
(6.2) \quad & G(1) = \{q\}, k = 1 \\
& \text{FOR } k = 1..g - 1 \text{ DO} \\
& G(k+1) = \bigcup_{z \in G(k) \cap X_\epsilon} \text{pre}\{z\}, k = k + 1 \\
& \text{END} \\
& \text{IF } w \in G(g) \text{ THEN} \\
& V(1) = G(g) \\
& \text{FOR } k = 1..g - 1 \text{ DO} \\
& V(k+1) = \left( \bigcup_{z \in V(k)} \text{succ}\{z\} \right) \cap (G(g+k)) \text{ END} \\
& \text{OTHERWISE} \\
& \text{FOR } h = 1..g \text{ DO } V(k) = \emptyset
\end{aligned}$$

**Proposition 6.2.** *Given  $M$ , a state  $q \in X_\epsilon$  is reached from  $w \in X \setminus X_\epsilon$  with a silent execution, and some of the states in this execution belong to the set  $\Omega$  if and only if there exists  $g \in [2, \lambda] : \left( \bigcup_{k=1..g} V(k) \right) \cap \Omega \neq \emptyset$ .*

*Proof.* Given the set  $\mathcal{S} \subset \mathcal{X}^*$  of all the finite silent executions  $x$  of  $M$ , of length  $g$ , with first state equal to  $w$  and last state equal to  $q$ , the recursion in equation (6.2) defines the sets  $V(k)$ ,  $k = 1..g$ . By construction,  $V(k) = \{q \in X : x(k) = q \wedge x \in \mathcal{S}\}$ . Therefore the result follows.  $\square$

On the basis of the above Propositions 6.1 and 6.2 and of the fact that after the execution of STEP 0 of Algorithm 1 the number of states in  $X$  is less than  $2N$ , where  $N$  is the original number of states of  $X$ , the following proposition holds:

**Proposition 6.3.** *The complexity of the Algorithm 1 is  $O(N^3)$ .*

*Proof.* Straightforward.  $\square$

We now establish a precise relationship between the FSM  $M$  and the FSM  $\widehat{M}$ . Recall that  $P(\sigma)$  is the projection of the string  $\sigma$ , i.e. the string obtained from  $\sigma$  by erasing the symbol  $\epsilon$ .

By construction,

- for any finite state execution  $x$  of  $M$  there exists a finite state execution  $\widehat{x}$  of  $\widehat{M}$ , such that  $\widehat{x} = P(x)$
- for any finite state execution  $x$  of  $M$  such that  $x(k) \notin \Omega, \forall k \in [1, |x|], \widehat{x}(k) \notin \widehat{\Omega}, \forall k \in [1, |\widehat{x}|], \widehat{x} = P(x)$
- for any finite state execution  $x$  of  $M$  for which there exists  $\delta \in [1, |x|]$  such that  $x(|x| - \delta) \in \Omega, \exists \widehat{\delta} \leq \delta : \widehat{x}(|\widehat{x}| - \widehat{\delta}) \in \widehat{\Omega}, \widehat{x} = P(x)$

Conversely,

- for any finite state execution  $\widehat{x}$  of  $\widehat{M}$  there exists a set of finite state executions  $x$  of  $M$ , such that  $P(x) = \widehat{x}$
- for any finite state execution  $\widehat{x}$  of  $\widehat{M}$  with  $\widehat{x}(k) \notin \widehat{\Omega}, \forall k \in [1, |\widehat{x}|], x(k) \notin \Omega, \forall k \in [1, |x|], \forall x : P(x) = \widehat{x}$
- given any finite state execution  $\widehat{x}$  of  $\widehat{M}$  for which there exists  $\delta \in [1, |\widehat{x}|]$  such that  $\widehat{x}(|\widehat{x}| - \delta) \in \widehat{\Omega}$ , for any finite state execution  $x$  of  $M$ , with  $P(x) = \widehat{x}$ , there exists  $\delta_x \geq \delta : x(|x| - \delta_x) \in \Omega$

Finally,

- $\mathbf{y}(\widehat{x}) = \mathbf{y}(x), \forall \widehat{x} = P(x)$
- $\mathbf{y}(x) = \mathbf{y}(\widehat{x}), \forall x : P(x) = \widehat{x}$

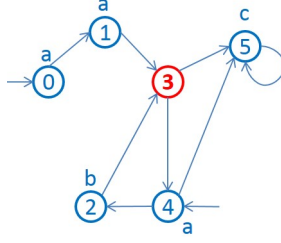
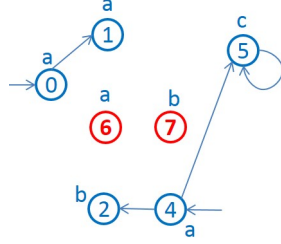
FIGURE 8. FSM  $M$ .

FIGURE 9. FSM after state space redefinition (STEP 1 of Algorithm 1).

Therefore we can establish the following result:

**Proposition 6.4.** *The FSMs  $M$  and  $\widehat{M}$  have the same output language. If  $M$  is parametrically  $\Omega$ -diag with parameters  $\tau, \delta, \gamma$  and  $T \in \{0, \infty\}$ , then there exist  $\widehat{\tau} \leq \tau, \widehat{\delta} \leq \delta, \widehat{\gamma} \leq \gamma$  such that  $\widehat{M}$  is parametrically  $\widehat{\Omega}$ -diag with parameters  $\widehat{\tau}, \widehat{\delta}, \widehat{\gamma}$  and  $\widehat{T} = T$ . Conversely, if  $\widehat{M}$  is parametrically  $\widehat{\Omega}$ -diag with parameters  $\widehat{\tau}, \widehat{\delta}, \widehat{\gamma}$  and  $\widehat{T} \in \{0, \infty\}$ , then there exist  $\tau \geq \widehat{\tau}, \delta \geq \widehat{\delta}$  and  $\gamma \geq \widehat{\gamma}$  such that  $M$  is parametrically  $\Omega$ -diag with parameters  $\tau, \delta, \gamma$  and  $T = \widehat{T}$ .*

**Example 6.5.** Consider the FSM  $M$  in Fig. 8, where the state 3 is critical (i.e.  $\Omega = \{3\}$ ) and silent (i.e.  $X_e = \{3\}$ ). Let  $X_0 = \{0, 4\}$ . By direct inspection  $M$  is eventually  $\Omega$ -diag, with  $\tau = 2$  and  $\delta = 1$ .

By applying Algorithm 1,  $X_F = \{1, 2\}$  and  $X_L = \{3\}$ . The state 3 is removed from the state space and substituted with the states called  $3_1, 3_2, (3_1, 1)$  and  $(3_2, 1)$ . Since there is no silent execution starting from  $w \in X_F$  and reaching the state 3 without crossing the set  $\Omega$ , then only  $(3_1, 1)$  and  $(3_2, 1)$  have to be considered. In Fig. 9 such states are renamed 6 and 7, respectively, for simplicity

After STEP 4, we obtain the FSM in Fig. 10.

Finally, we can remove the sink states 1 and 2, and the resulting FSM  $\widehat{M}$  is depicted in Fig. 11, and  $\widehat{\Omega} = \{6, 7\}$ . Then  $\widehat{M}$  is eventually  $\widehat{\Omega}$ -diag, with  $\widehat{\tau} = 1 \leq \tau$  and  $\widehat{\delta} = 1 \leq \delta$ , in accord to Proposition 6.4

In the following table we see how state trajectories of  $M$  are mapped on state trajectories of  $\widehat{M}$ .

$x$	$\widehat{x}$	$y(x) = y(\widehat{x})$
0135*	065*	aac*
013(423)*5*	06(47)*5*	aa(ab)*c*
01345*	0645*	ac*
4(234)*5*	4(74)*5*	a(ab)*c*
4235*	475*	abc*
45*	45*	ac*

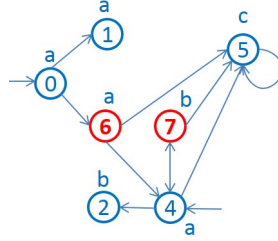
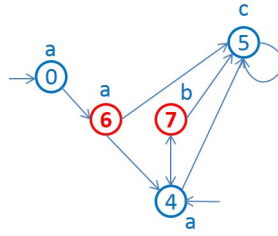


FIGURE 10. FSM after STEP 4 (Algorithm 1).

FIGURE 11. FSM  $\widehat{M}$ .

## 7. CONCLUSIONS

In this paper, we proposed a general framework for the analysis and characterization of observability and diagnosability of finite state systems. Observability and diagnosability were defined with respect to a subset of the state space, called critical set, i.e. a set of discrete states representing a set of faults, or more generally any set of interest. Using the proposed framework, it is possible to check diagnosability of a critical event and at the same time compute the delay of the diagnosis with respect to the occurrence of the event, the uncertainty about the time at which that event occurred, and the duration of a possible initial transient where the diagnosis is not possible or nor required. Moreover, in the unifying framework we propose, it was possible to precisely compare some of observability and diagnosability notions existing in the literature and the ones we introduced in our paper.

For discrete event systems, some effort in the direction of a decentralized approach to observability and diagnosability has been made e.g. in [5] and in [24] where the observability with respect to a language [18] was generalized to the case of decentralized systems by introducing the notion of coobservability. In [32] and in [34] it was proven that coobservability and codiagnosability can be mapped from one to the other. Extending our approach to a decentralized framework and comparing our results with the ones above will be the subject of future investigation.

## REFERENCES

- [1] M. Babaali and G.J. Pappas. Observability of switched linear systems in continuous time. In L. Thiele M. Morari and F. Rossi, editors, *Hybrid Systems: Computation and Control 2005*, volume 3414 of *Lecture Notes in Computer Science*, pages 103–117. Springer-Verlag, 2005.
- [2] A. Balluchi, L. Benvenuti, M. D. Di Benedetto, and A. Sangiovanni-Vincentelli. The design of dynamical observers for hybrid systems: Theory and application to an automotive control problem. *Automatica*, 49:915–925, 2013.
- [3] A. Balluchi, L. Benvenuti, M. D. Di Benedetto, and A.L. Sangiovanni-Vincentelli. Design of observers for hybrid systems. In C.J. Tomlin and M.R. Greensreer, editors, *Hybrid Systems: Computation and Control*, volume 2289 of *Lecture Notes in Computer Science*, pages 76–89. Springer Verlag, 2002.



- [4] A. Bemporad, G. Ferrari-Trecate, and M. Morari. Observability and controllability of piecewise affine and hybrid systems. *IEEE Trans. Automatic Control*, 45 (10):1864–1876, 2000.
- [5] R. Cieslak, C. Desclaux, A.S. Fawaz, and P. Varaiya. Supervisory control of discrete-event processes with partial observations. *IEEE Trans. Automatic Control*, 33(3):249–260, 1988.
- [6] P. Collins and J.H. van Schuppen. Observability of piecewise-affine hybrid systems. In R. Alur and G.J. Pappas, editors, *Hybrid Systems: Computation and Control (HSCC'04)*, volume 2993 of *Lecture Notes in Computer Science*, pages 265–279. Springer, 2007.
- [7] E. De Santis and M.D. Di Benedetto. Observability of hybrid dynamical systems. *Foundations and Trends in Systems and Control (to appear)*, 00:0–0, 2016.
- [8] E. De Santis, M.D. Di Benedetto, S. Di Gennaro, A. D’Innocenzo, and G. Pola. Critical observability of a class of hybrid systems and application to air traffic management. In H. A.P. Blom and J. Lygeros, editors, *Stochastic Hybrid Systems: Theory and Safety Critical Applications*, volume 337 of *Lecture Notes in Control and Information Sciences*, pages 141–170. Springer-Verlag, 2006.
- [9] E. De Santis, M.D. Di Benedetto, and G. Pola. On observability and detectability of continuous-time linear switching systems. In *Proceedings of the 42<sup>nd</sup> IEEE Conference on Decision and Control, CDC 03, Maui, Hawaii, USA*, pages 5777–5782, December 2003.
- [10] E. De Santis and M.D. Di Benedetto (Eds.). Special issue on observability and observer-based control of hybrid systems. *Int. J. Robust Nonlinear Control*, 19:1519–1520, 2009.
- [11] M. D. Di Benedetto, S. Di Gennaro, and A. D’Innocenzo. Critical observability and hybrid observers for error detection in air traffic management. In *Proceedings of 13<sup>th</sup> Mediterranean Conference on Control and Automation, Limassol, Cyprus*, 2005.
- [12] M. D. Di Benedetto, S. Di Gennaro, and A. D’Innocenzo. Error detection within a specific time horizon and application to air traffic management. In *Proceedings of the Joint 44<sup>th</sup> IEEE Conference on Decision and Control and European Control Conference (CDC-ECC’05), Seville, Spain*, pages 7472–7477, December 2005.
- [13] E. W. Griffith and K. S. P. Kumar. On the observability of nonlinear systems. *J. Math. Anal. Appl.*, 1971.
- [14] S. Hashtrudi Zad, R. H. Kwong, and W. M. Wonham. On the observability of nonlinear systems. *J. Math. Anal. Appl.*, 1971.
- [15] R. E. Kalman. On the general theory of control systems. *IRE Transactions on Automatic Control*, 4(3):481–492, 1959.
- [16] S. Lafortune. On decentralized and distributed control of partially-observed discrete event systems. In C. Bonivento et al., editor, *Adv. in Control Theory and Applications*, volume 353 of *(LNCIS)*, pages 171–184. Springer, 2007.
- [17] F. Lin. Diagnosability of discrete event systems and its applications. *Discrete Event Dynamic Systems*, 4 (1):197–212, 1994.
- [18] F. Lin and W.M. Wonham. On observability of discrete-event systems. *Information Sciences*, 44:173–198, 1988.
- [19] D.G. Luenberger. An introduction to observers. *IEEE Trans. on Automatic Control*, 16(6):596–602, 1971.
- [20] C.M. Ozveren and A.S. Willsky. Observability of discrete event dynamic systems. *IEEE Transactions on Automatic Control*, 35(7):797–806, 1990.
- [21] G. Pola, D. Pezzuti, E. De Santis, and M.D. Di Benedetto. Design of decentralized critical observers for networks of finite statemachines: A formal method approach. *submitted*, 2016.
- [22] P. J. Ramadge and W. M. Wonham. The control of discrete-event systems. *Proc. IEEE*, 77(1):81–98, 1989.
- [23] P.J. Ramadge. Observability of discrete event systems. In *Proceedings of the 25<sup>th</sup> IEEE Conference on Decision and Control, Athens, Greece*, pages 1108–1112, December 1986.
- [24] K. Rudie and W. Wonham. Think globally, act locally: decentralized supervisor control. *IEEE Trans. Autom. Control*, 37(11):1692–1708, 1989.
- [25] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis. Diagnosability of discrete-event systems. *IEEE Transactions on Automatic Control*, 40(9):1555–1575, 1995.
- [26] D. Sears and K. Rudie. On computing indistinguishable states of nondeterministic finite automata with partially observable transitions. In *Proceedings of the 53rd IEEE Conference on Decision and Control, Los Angeles, California, USA*, pages 6731–6736, 2014.
- [27] S. Shu and F. Lin. Delayed detectability of discrete event systems. *IEEE Trans. on Automatic Control*, 58(4):862–875, 2013.
- [28] S. Shu, F. Lin, and H. Ying. Detectability of discrete event systems. *IEEE Trans. on Automatic Control*, 52(12):2356–2359, 2007.
- [29] S. Takai and T. Ushio. Verification of codiagnosability for discrete event systems modeled by mealy automata with non-deterministic output functions. *IEEE Trans. Autom. Control*, 57(3):798–804, 2012.
- [30] A. Tanwani, H. Shim, and D. Liberzon. Observability for switched linear systems: Characterization and observer design. *IEEE Trans. Autom. Control*, 58(4):891–904, 2013.
- [31] R. Vidal, A. Chiuso, S. Soatto, and S. Sastry. Observability of linear hybrid systems. In A. Pnueli and O. Maler, editors, *Hybrid Systems: Computation and Control*, volume 2623 of *Lecture Notes in Computer Science*, pages 526–539. Springer Verlag, 2003.
- [32] W. Wang, A.R. Girard, and S. Lafortune. On codiagnosability and coobservability with dynamic observations. *IEEE Transactions on automatic control*, 56(7):1551–1566, 2011.
- [33] W. Wang, S. Lafortune, and F. Lin. An algorithm for calculating indistinguishable states and clusters in finite-state automata with partially observed transitions. *Systems & Control Letters*, pages 656–661, 2007.

- [34] X. Yin and S. Lafortune. Codiagnosability and coobservability under dynamic observations: Transformations and verifications. *Automatica*, 61:241–252, 2015.
- [35] J. Zaytoon and S. Lafortune. Overview of fault diagnosis methods for discrete event systems. *Annual Reviews in Control*, 37:308–320, 2013.

<sup>1</sup>DEPARTMENT OF INFORMATION ENGINEERING, COMPUTER SCIENCE AND MATHEMATICS, CENTER OF EXCELLENCE DEWS, UNIVERSITY OF L'AQUILA, 67100 L'AQUILA, ITALY

*E-mail address:*    `{elena.desantis,mariadomenica.dibenedetto}@univaq.it`